BY ORDER OF THE SECRETARY OF THE AIR FORCE

AIR FORCE INSTRUCTION 33-332

5 JUNE 2013

Communications and Information

THE AIR FORCE PRIVACY AND CIVIL LIBERTIES PROGRAM

COMPLIANCE WITH THIS PUBLICATION IS MANDATORY

ACCESSIBILITY: Publications and forms are available for downloading or ordering on the e-Publishing website at **www.e-publishing.af.mil.**

RELEASABILITY: There are no releasability restrictions on this publication.

OPR: SAF/A6PPF

Certified by: SAF/A6P (Dr. Fred P. Lewis)

Supersedes: AFI33-332, 16 May 2011

Pages: 74

This Instruction implements Public Law 110-53 (42 U.S.C. § 2000ee-1) Section 803; Air Force Policy Directive (AFPD) 33-3, *Information Management*; Department of Defense Directive (DoDD) 5400.11, *Department of Defense Privacy Program*; Department of Defense Instruction (DoDI) 5400.16, *DoD Privacy Impact Assessment (PIA) Guidance;* DoDI 1000.30, *Reduction of Social Security Number (SSN) Use Within DoD*; and DoDI 1000.29, *DoD Civil Liberties Program.* The Instruction provides guidance for collecting, safeguarding, maintaining, using, accessing, amending and disseminating Personally Identifiable Information (PII) in Air Force Privacy Act and other records, whether in paper or electronic format and guidance on the Air Force Civil Liberties Program, to include training personnel about (Civil Liberties) and reporting Civil Liberties complaints. In addition to this instruction, Air Force medical organizations that meet the definition of a covered entity must also comply with the Health Insurance Portability and Accountability Act (HIPAA), as required by DoD 6025.18-R, *DoD Health Information Privacy Regulation;* DoD 8580.02-R, *DoD Health Information Security Regulation;* and Air Force Instruction (AFI) 41-210, *TRICARE Operations and Patient Administration Functions,* which covers protected health information (PHI) held by them. This Instruction applies to Air Force Active Duty, Air Reserve Command (AFRC) and Air National Guard (ANG) units, government civilians, contractors and Civil Air Patrol when performing functions for the Air Force, and in accordance with (IAW) DoDD 5100.3, *Support of the Headquarters of Combatant and Subordinate Joint Commands*. Air National Guard personnel not in a federal status are subject to their respective state military code or applicable administrative actions, as appropriate. Ensure that all records created as a result of processes prescribed in this Instruction are maintained in accordance with Air Force Manual (AFMAN) 33-363, *Management of Records,* and disposed of in accordance with the Air Force Records Disposition Schedule (RDS) maintained in the Air Force Records Information Management System (AFRIMS) located at

https://www.my.af.mil/afrims/afrims/afrims/rims.cfm. Refer recommended changes and questions about this Instruction to the Office of Primary Responsibility (OPR) using the AF Form 847, *Recommendation for Change of Publication*; route through the appropriate functional chain of command. Send supplements and implementing publications of this Instruction to the Chief Information Dominance and Chief Information Officer (SAF/CIO A6), 1800 Air Force Pentagon, Washington, DC 20330-1800 for review and coordination prior to publication. The terms "must", "shall", and "will" denote mandatory actions in this instruction.

This Instruction requires collecting and maintaining information protected by the *Privacy Act of 1974*, System of Records Notices (SORN) F033 AF B, *Privacy Act Request File*, and F036 AF PC Q, *Personnel Data Systems (PDS)*, apply.

Personnel who fail to adhere to this Instruction; specifically paragraphs 1.1.11.1 and 1.1.11.4, may be punished under Uniform Code of Military Justice (UCMJ) Article 92(1) or civil equivalent.

Article 92(1) of the UCMJ does not apply to the Air National Guard (ANG) while in Title 32 status, however, the State UCMJ equivalent may apply.

SUMMARY OF CHANGES

This instruction has been substantially changed and must be completely reviewed. Changes include incorporating the Civil Liberties Programs.

Chapter 1—OVERVIEW OF THE PRIVACY PROGRAM **6**

1.1. Basic Guidelines. 6

1.2. Responsibilities. 11

1.3. Personally Identifiable Information (PII). 15

1.4. Privacy Complaints and Violations. 15

Chapter 2—COLLECTING PERSONAL INFORMATION FROM INDIVIDUALS **17**

2.1. Each agency that maintains a SOR shall: 17

2.2. Privacy Notifications and Safeguards. 17

2.3. Social Security Number (SSN) Reduction Plan. 19

Chapter 3—FIRST PARTY ACCESS TO OWN RECORDS UNDER THE PRIVACY ACT **22**

3.1. Making a Request for Access. 22

3.2. Processing a Request for Access. 22

3.3. Fees. 22

3.4. Do not charge fees: 22

3.5. Denying or Limiting Access. 23

3.6. Denial Authorities. 23

Chapter 4—AMENDING A PRIVACY ACT RECORD 25

4.1. Amendment Reasons. 25

4.2. Responding to Amendment Requests. 25

4.3. Approving or Denying a Record Amendment. 25

4.4. Contents of Privacy Act Processing Case Files. 25

Chapter 5—APPEALS 26

5.1. Appeal Procedures. 26

Chapter 6—DISCLOSING RECORDS TO THIRD PARTIES 27

6.1. Disclosure Considerations. 27

6.2. Releasable Information. 28

6.3. Disclosing Information. 29

6.4. Rules for Releasing Privacy Act Information Without Consent of the Subject. 29

6.5. Disclosing the Medical Records of Minors. 29

6.6. Disclosure Accountings. 30

6.7. Computer Matching. 30

6.8. Privacy and the Web. 31

Chapter 7—PRIVACY IMPACT ASSESSMENTS 32

7.1. Evaluating Information Systems for Privacy Act Compliance and Risk Identification. 32

7.2. What is a PIA? The Privacy Impact Assessment is an analysis of how PII information is collected and handled in an IT system: 32

7.3. When a PIA is required. 32

7.4. When a PIA is not required. 33

7.5. Who conducts the PIA? The ISO shall conduct a PIA in conjunction with the system PM, IAM and local/functional Privacy Manager. 33

7.6. Format and Digital Signatures. 33

7.7. Submitting Approved PIAs. 33

Chapter 8—PREPARING SYSTEM OF RECORDS NOTICE (SORN) FOR PUBLISHING IN THE FEDERAL REGISTER 34

8.1. Publishing System of Records Notices (SORNs). 34

8.2. When is a SORN required? A SORN is required when information onan individual is retrieved by name of the indivdiual; some identifying number, symbol, or other identifying particular assigned to the individual. 34

8.3. Adopting Existing SORNs. 34
8.4. Updating SORNs. 35
8.5. Submitting SORNs for Publication in the Federal Register. 35
8.6. Requirement for Periodic review of published SORNs. 35
8.7. Deletion of SORNs. 35

Chapter 9—PROTECTING AND DISPOSING OF RECORDS 36

9.1. Protecting Records. 36
9.2. Guidance on Protecting PII. 36
9.3. PII Breach Reporting. 38
9.4. Risk Based Management. 40
9.5. Disposing of Records. 40

Chapter 10—PRIVACY ACT EXEMPTIONS 41

10.1. Exemption Types. 41
10.2. Authorizing Exemptions. 41
10.3. Requesting an Exemption. 41
10.4. Exemptions. 41

Chapter 11—PRIVACY ACT TRAINING 43

11.1. Who Needs Training. 43
11.2. Privacy Act Training Tools. 44

CHAPTER 12—CIVIL LIBERTIES 45

12.1. Basic Guidelines. 45
12.2. Civil Liberties. 45
12.3. Responsibilities. 45
12.4. Civil Liberties Quarterly Report. 47
12.5. Reprisal For Making Complaint: 48
12.6. Who Needs Training. 48
12.7. Civil Liberties Training Tools. 48

Attachment 1—GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION 50

Attachment 2—PREPARING A SYSTEM OF RECORDS NOTICE (SORN) 58

Attachment 3—DOD BLANKET ROUTINE USE 60

Attachment 4—ALTERING A SYSTEM OF RECORD NOTICE 63

Attachment 5—RISK ASSESSMENT 65

Attachment 6—PREPARING A DOD SSN JUSTIFICATION MEMORANDUM 66

Attachment 7—EXAMPLE PRIVACY BREACH NOTIFICATION LETTER 67

Attachment 8—APPROVED DOD TRAINING WEBSITES 68

Attachment 9—NATIONAL COMPLAINT VIGNETTES 69

Attachment 10—CIVIL LIBERTIES COMPLAINT REPORT INSTRUCTIONS 72

Attachment 11—EXAMPLE CIVIL LIBERTIES REPORT 74

Chapter 1

OVERVIEW OF THE PRIVACY PROGRAM

1.1. Basic Guidelines.

1.1.1. The Privacy Act of 1974, 5 U.S.C. § 552a, The Congress finds the following:

(1) The privacy of an individual is directly affected by the collection, maintenance, use, and dissemination of personal information by Federal agencies;

(2) The increasing use of computers and sophisticated information technology, while essential to the efficient operations of the Government, has greatly magnified the harm to individual privacy that can occur from any collection, maintenance, use, or dissemination of personal information;

(3) The opportunities for an individual to secure employment, insurance, and credit, and his right to due process, and other legal protections are endangered by the misuse of certain information systems;

(4) The right to privacy is a personal and fundamental right protected by the Constitution of the United States; and

(5) In order to protect the privacy of individuals identified in information systems maintained by Federal agencies, it is necessary and proper for the Congress to regulate the collection, maintenance, use, and dissemination of information by such agencies.

1.1.2. The purpose of this Act is to provide certain safeguards for an individual against an invasion of personal privacy by requiring Federal agencies, except as otherwise provided by law, to:

(1) Permit an individual to determine what records pertaining to him/her are collected, maintained, used, or disseminated by such agencies;

(2) Permit an individual to prevent records pertaining to him/her obtained by such agencies for a particular purpose from being used or made available for another purpose without his/her consent;

(3) Permit an individual to gain access to information pertaining to him/her in Federal agency records, to have a copy made of all or any portion thereof, and to correct or amend such records;

(4) Collect, maintain, use, or disseminate any record of identifiable personal information in a manner that assures that such action is for a necessary and lawful purpose, that the information is current for its intended use, and that an accurate adequate safeguards are provided to prevent misuse of such information;

(5) Permit exemptions from the requirements with respect to records provided in this Act only in those cases where there is an important public policy need for such exemption as has been determined by specific statutory authority; and

(6) Be subject to civil suit for any damages which occur as a result of willful or intentional action which violates any individual's rights under this Act.

1.1.3. The E-Government Act of 2002, 44 U.S.C. 3601, Congress finds the following:

(1) The use of computers and the Internet is rapidly transforming societal interactions and the relationships among citizens, private businesses, and the Government.

(2) The Federal Government has had uneven success in applying advances in information technology to enhance governmental functions and services, achieve more efficient performance, increase access to Government information, and increase citizen participation in Government.

(3) Most Internet-based services of the Federal Government are developed and presented separately, according to the jurisdictional boundaries of an individual department or agency, rather than being integrated cooperatively according to function or topic.

(4) Internet-based Government services involving interagency cooperation are especially difficult to develop and promote, in part because of a lack of sufficient funding mechanisms to support such interagency cooperation.

(5) Electronic Government has its impact through improved Government performance and outcomes within and across agencies.

(6) Electronic Government is a critical element in the management of Government, to be implemented as part of a management framework that also addresses finance, procurement, human capital, and other challenges to improve the performance of Government.

(7) To take full advantage of the improved Government performance that can be achieved through the use of Internet based technology requires strong leadership, better organization, improved interagency collaboration, and more focused oversight of agency compliance with statutes related to information resource management.

1.1.4. The purposes of this Act are the following:

(1) To provide effective leadership of Federal Government efforts to develop and promote electronic Government services and processes by establishing an Administrator of a new Office of Electronic Government within the Office of Management and Budget.

(2) To promote use of the Internet and other information technologies to provide increased opportunities for citizen participation in Government.

(3) To promote interagency collaboration in providing electronic Government services, where this collaboration would improve the service to citizens by integrating related functions, and in the use of internal electronic Government processes, where this collaboration would improve the efficiency and effectiveness of the processes.

(4) To improve the ability of the Government to achieve agency missions and program performance goals.

(5) To promote the use of the Internet and emerging technologies within and across Government agencies to provide citizen-centric Government information and services.

(6) To reduce costs and burdens for businesses and other Government entities.

(7) To promote better informed decision making by policy makers.

(8) To promote access to high quality Government information and services across multiple channels.

(9) To make the Federal Government more transparent and accountable.

(10) To transform agency operations by utilizing, where appropriate, best practices from public and private sector organizations.

(11) To provide enhanced access to Government information and services in a manner consistent with laws regarding protection of personal privacy, national security, records retention, access for persons with disabilities, and other relevant laws.

1.1.5. Personal information is defined by the Department of Defense (DoD) as "information about an individual that identifies, links, relates, or is unique to, or describes him or her, e.g., social security number (SSN); age; military rank; civilian grade; marital status; race; salary; home/office phone numbers; other demographic, biometric, personnel, medical, and financial information, etc. Such information is also known as personally identifiable information (PII) (i.e., information which can be used to distinguish or trace an individual's identity, such as their name, social security number, date of birth, place of birth, mother's maiden name, or biometric records, including any other PII which is linked or linkable to a specified individual)."

1.1.6. The Privacy Act, defines the term record as "any item, collection, or grouping of information about an individual that is maintained by an agency, including, but not limited to, education, financial transactions, medical history, and criminal or employment history and that contains name, or the identifying number, symbol, or other identifying particular assigned to the individual, such as a finger or voice print or a photograph."

1.1.7. The Federal Records Act, 44 U.S.C. § 3301, defines a federal government record as "all books, papers, maps, photographs, machine readable materials, or other documentary materials, regardless of physical form or characteristics, made or received by an agency of the United States Government under Federal law or in connection with the transaction of public business and preserved or appropriate for preservation by that agency or its legitimate successor as evidence of the organization, functions, guidance, decisions, procedures, operations, or other activities of the Government or because of the informational value of data in them." The definition of a record for purposes of the Federal Records Act is broader than as defined under the Privacy Act.

1.1.8. Records that are retrieved by name or other personal identifier of a U.S. citizen or a person lawfully admitted for permanent residence are subject to requirements of the Privacy

Act of 1974 and are referred to as a system of records (SOR). The DoD defines a system of records (SOR) as "a group of records, whatever the storage media (paper, electronic, etc.), under the control of a DoD Component from which personal information about an individual is retrieved by the name of the individual, or by some other identifying number, symbol, or other identifying particular assigned, that is unique to the individual." SORs are only authorized as necessary to conduct the Air Force mission. The authority to establish a SOR must be derived from a specific statute or Executive Order that authorizes maintaining information in a system of records (IAW DoD 5400-11.R, *Department of Defense Privacy Program).*

1.1.9. System of Records Notices (SORN), also referred to as Privacy Act System of Records Notices, are legal documents that describe the kinds of records collected and maintained in a SOR, on whom they are maintained, what the records are used for, and how an individual may access or contest the records in the system. DoD requires a SORNs for SORs being maintained by the AF to be published in the *Federal Register* to allow the general public a 30 day opportunity to comment before changing or implementing a SOR. Procedures for SORNs are addressed in Chapter 8 of this Instruction.

1.1.10. Air Force personnel or supporting contractors *shall*:

1.1.10.1. Only maintain paper and/or electronic SOR under the authority of an approved SORN which has been published in the *Federal Register*.

1.1.10.2. Only collect, maintain, and use information under such systems for purposes described in the published SORN to support programs authorized by law or executive order and as implemented by DoD and AF prescribing directives.

1.1.10.3. Safeguard the records in the system, keep them the minimum time required, and dispose of them according to Records Disposition Schedule (RDS).

1.1.10.4. Ensure records are timely, accurate, relevant, and completed.

1.1.10.5. Amend and correct information in SOR upon request, as appropriate.

1.1.10.6. Allow individuals to review and receive copies of their own records unless an exemption published in the *Federal Register* applies. (See Chapter 10 or **http://dpclo.defense.gov/privacy/SORNs/SORNs.html#exemp**).

1.1.10.7. Ensure personal information maintained in electronic files or folders are not stored on SharePoint or equivalent or like software programs unless required for daily operation and is accessible to only those individuals who have an official valid "need-to-know".

1.1.10.8. Remove personal information maintained within SharePoint or equivalent or like software programs when no longer needed for daily operations and file IAW AF RDS.

1.1.10.9. Ensure personal information stored on share drives is only accessible to individuals who have an official valid "need-to-know".

1.1.10.10. Use the Army Missile Research Development and Engineering Center Safe Access File Exchange (AMRDEC SAFE) as an alternate means of transmitting PII (does not apply for transmitting Protect Health Information (PHI)) to personal or commercial e-mail accounts

(**https://safe.amrdec.army.mil/SAFE2/**). 1.1.10.11. Use official forms and similar tools that have been approved and published IAW AFI 33-360, *Publications and Forms Management,* when collecting personal information. (See paragraph 1.2.6.2).

1.1.10.11. Request for an Office Management and Budget control number whenever information is being collected from the general public. For the purpose of this requirement, contractors are considered part of the general public. See AFI 33-324, *The Information Collections and Reports Management Program: Controlling Internal, Public, and Interagency Air Force Information Collections.*

1.1.11. Air Force personnel or supporting contractors *shall not*:

1.1.11.1. Maintain system of records on individuals without their knowledge and/or having a SORN published to the *Federal Register*. Personnel who fail to adhere to this paragraph may be punished under Uniform Code of Military Justice (UCMJ) Article 92(1) or civil equivalent.

1.1.11.2. Keep records on how a person exercises First Amendment rights. First Amendment rights include, but are not limited to, freedom of religion, freedom of political beliefs, freedom of speech, freedom of the press, the right to assemble, and the right to petition. *EXCEPTIONS are when*: The Air Force has the permission of that individual, the individual posts/sends the record directly to the Air Force, or is authorized by Federal statute; or the information pertains to and is within the scope of an authorized law enforcement activity.

1.1.11.3. Penalize or harass an individual for exercising rights guaranteed under the Privacy Act.

1.1.11.4. Transmit informational material or communications that contains individuals' SSN, Financial Information, Driver License, Passport or Alien Registration Number to or from personal or commercial e-mail accounts unless a written consent has been submitted by the individual who has requested their personal information to be sent to their personal or commercial e-mail account. In addition, transmitting of PHI is prohibited. Personnel who fail to adhere to this paragraph may be punished under Uniform Code of Military Justice (UCMJ) Article 92(1) or civil equivalent.

1.1.11.5. Use auto-forwarding through multiple user accounts to circumvent CAC-based authentication and DoD encryption requirements.

1.1.11.6. Mail or courier sensitive PII on CDs, DVDs, hard drives, flash drives, floppy disks or other removable media unless the data is encrypted (see AFI 33-200, *Information Assurance Management*).

1.1.11.7. Return failed hard drives to include copiers with internal hard drives to vendor for warranty if the device was ever used to store sensitive PII, without ensuring all data has been permanently removed.

1.1.11.8. Leave personal information in unsecured vehicles, unattended workspaces, unsecured file drawers, or in checked baggage.

1.1.11.9. Store and/or use personal information on personal media.

1.1.11.10. File personal notes in a SOR, as personal notes will be considered part of the SOR.

1.2. Responsibilities.

1.2.1. The Chief, Information Officer (SAF/CIO A6) shall:

1.2.1.1. Establish procedures to ensure compliance with the Privacy Act and the DoD privacy program.

1.2.1.2. Appoint a Component Senior Official for Privacy (CSOP) with overall responsibility for the Air Force privacy program.

1.2.1.3. Appoint an AF Privacy Officer with responsibility for implementing the AF privacy program.

1.2.2. The CSOP shall:

1.2.2.1. Ensure DoD and AF proposals, policies, or programs having privacy implications are evaluated to ensure consistency with privacy principles.

1.2.2.2. Ensure the AF privacy program is periodically reviewed by the Inspector General (IG) or other officials, who have specialized knowledge of the privacy policies.

1.2.2.3. Supervise and oversee management of the AF Privacy Program as administered by the Air Force Privacy Officer.

1.2.2.4. The CSOP or the AF Privacy Officer will serve as the AF representative on the Defense Privacy Board and the Defense Data Integrity Board, which are administered through the Defense Privacy and Civil Liberties Office (DPCLO).

1.2.3. The Air Force Privacy Officer shall:

1.2.3.1. Administer guidance and procedures prescribed in this Instruction.

1.2.3.2. Develop AF policy to ensure protection of Personal and Personally Identifiable Information (PII).

1.2.3.3. Provide guidance and assistance to Privacy Managers.

1.2.3.4. Conduct mandatory reviews of publications and forms for compliance with this Instruction.

1.2.3.5. Review Privacy Impact Assessments (PIA) for submission to SAF/CIO A6 for approval (see Chapter 7).

1.2.3.6. Review and approve proposed new, altered, amended, and deleted SORNs.

1.2.3.7. Report Privacy Breaches to the DPCLO within the prescribed timelines. Track and monitor breach trends to improve guidance and procedures (see Chapter 9).

1.2.3.8. Ensure privacy training and training tools are available for a variety of AF audiences (see Chapter 11).

1.2.3.9. Prepare and submit reports as required to DPCLO.

1.2.3.10. Provide guidance and support to the field to ensure information systems which are developed to collect, maintain, process, or disseminate personal information or PII conform to the Privacy Act, OMB, DoD, and AF requirements.

1.2.3.11. Coordinate with SAF/A6OI, Information Assurance Division, to ensure appropriate Information Assurance Control procedures are applied by Information System Owners (ISO), Program Managers (PM), Information Assurance Managers (IAM), and Portfolio Managers during the Certification and Accreditation (C&A) process to protect Privacy Act information throughout the IT system life cycle.

1.2.3.12. Serve as the AF representative on the Defense Privacy Board and the Defense Data Integrity Board, which are administered through the Defense Privacy and Civil Liberties Office (DPCLO).

1.2.4. The Deputy General Counsel (Fiscal, Ethics and Administrative Law) to the Secretary of the Air Force (SAF/GCA) shall make final decisions on Privacy Act appeals. AFLOA/JACL receives Privacy Act appeals and provides recommendations to the appellate authority. Service unique appeals, from unified combatant commands, should go through the respective service component chain of command.

1.2.5. The Office of The Judge Advocate General, Administrative Law Directorate (AF/JAA), and Judge Advocate legal offices shall provide advice to the Privacy Officer/Manager/Monitor, commanders, and supervisors on requests made under the Privacy Act and the Freedom of Information Act.

1.2.6. AF Departmental Forms Management Officer shall:

1.2.6.1. Maintain a database of both new and existing forms reviewed to produce an annual report every July 1. This report shall be submitted to the AF Privacy Officer as input into the Privacy section of the annual Federal Information Security Management Act (FISMA) report as required by Subchapter III, Chapter 35 of Title 44, United States Code (see paragraph 2.3).

1.2.6.2. Ensure OPRs for new and revised forms that collect personal information which will be maintained in a SOR, coordinate with the supporting Privacy Manager/Monitor before publishing. Final publishing packages must contain a completed AF Form 673, Air Force Publication/Form Action Request, IAW AFI 33-360, *Publications and Forms Management*; and if applicable, the associated SORN and Defense Privacy Civil Liberties Office (DPCLO) approved SSN justification memo (see paragraph 2.3).

1.2.7. MAJCOM/A6s and Communication Squadron Commanders shall:

1.2.7.1. Establish a Privacy Office within the A6 community and appoint in writing a Privacy Manager/Monitors to execute command and base-level responsibilities as outlined in this Instruction.

1.2.7.2. Establish policies necessary to implement and enforce the AF privacy program.

1.2.7.3. Ensure all assigned AF personnel are aware of and understand the requirements within this Instruction.

1.2.7.4. Ensure all assigned personnel have completed required mandatory annual and specialize privacy training.

1.2.8. HAF/MAJCOM/FOA/DRU/Base Privacy Managers/Monitors shall:

1.2.8.1. Provide guidance and training to commanders and personnel implementing this Instruction.

1.2.8.2. Promote privacy awareness throughout the organization and assist commanders with establishing procedures to reinforce the protection of personal information or PII.

1.2.8.3. Report privacy breaches and provide guidance to organizations where the breach occurred.

1.2.8.4. Provide guidance to assist with resolution of privacy complaints and violations.

1.2.8.5. Review and process Privacy Act Request denial recommendations.

1.2.8.6. Track assigned personnel privacy training.

1.2.8.7. Provide specialized training to individuals who handle privacy information on a daily or routine basis in addition to Privacy Act Annual Refresher training. (See Chapter 11).

1.2.8.8. Review organizational publications and forms for compliance with this Instruction (see paragraph 1.2.7.2).

1.2.8.9. Provide updates as needed of Privacy Manager/Monitor names, office symbols, voice number, FAX number, unclassified e-mail addresses to the Privacy Manager in their chain of command who in turn shall forward a copy to the Air Force Privacy Officer (SAF/A6PPF) for continuity.

1.2.8.10. Submit quarterly reports and/or other required reports as directed by the AF Privacy Officer. Quarterly reports may consist of the number of SORNs reviewed, privacy complaints, and training provided.

1.2.8.11. Conduct Staff Assistance Visits (SAVs)/Command Unit Inspections as necessary to ensure compliance and health of privacy programs.

1.2.8.12. Provide guidance to ISO, PM and IAM for completing a SORNs and PIAs for IT systems.

1.2.8.13. Assist ISO/PM with reviewing SORNs and PIAs annually to coincide with the IT system review cycle for C&A and FISMA reviews. Coordination and teamwork are required between ISO, PM, IAM and Privacy Managers.

1.2.9. Organizational Commanders and Equivalents shall: (Examples of commander equivalents include Director of Staff, Civilian Director of an organization, or a Commandant of a school).

1.2.9.1. Appoint a Unit Privacy Monitor in writing and submit to the base Privacy Manager.

1.2.9.2. Reinforce the importance of safeguarding PII and ensure personnel who fail to safeguard PII are counseled or disciplined as appropriate.

1.2.9.3. Direct an inquiry to determine the circumstances and impact of privacy breaches IAW Chapter 9 of this Instruction.

1.2.9.4. Ensure coordination and teamwork is accomplished between ISO, PM, IAMs and Privacy Managers.

1.2.9.5. Ensure all assigned AF personnel are aware of and understand the requirements within this Instruction.

1.2.9.6. Ensure additional privacy training is incorporated into in-house training.

1.2.10. Unit Privacy Monitors shall:

1.2.10.1. Provide guidance and training to commanders and personnel implementing this Instruction.

1.2.10.2. Promote privacy awareness throughout the organization and assist commanders/equivalent with implementing procedures to reinforce the protection of PII.

1.2.10.3. Track assigned personnel requiring privacy training.

1.2.10.4. Provide specialized training to individuals who handle privacy information on a daily or routine basis in addition to Privacy Act Annual Refresher training (see Chapter 11).

1.2.10.5. Review organizational publications and forms for compliance with this Instruction.

1.2.10.6. Provide guidance to the commander/equivalent to assist with resolution of privacy breaches, complaints, and violations.

1.2.10.7. Submit quarterly reports and/or other required reports as directed by the Privacy Manager.

1.2.11. Functional Level ISOs, PMs, and IAMs shall:

1.2.11.1. Implement privacy safeguards, complete PIAs and SORNs. Guidance may be provided by supporting Privacy Manager (see Chapter and DoDI 5400.16, *DoD Privacy Impact Assessment (PIA) Guidance*).

1.2.11.2. Determine early in the design phase of IT systems what personal information will be collected, used, processed, stored, or disseminated in the electronic systems of records.

1.2.11.3. Formulate Privacy Act requirements in early stages of IT systems design, development, and data management to plan for and implement Information Assurance (IA) controls to safeguard PII.

1.2.11.4. Ensure records containing PII are safeguarded or removed as required from all IT systems prior to disposal, replacement, or reuse of IT hardware storage components (hard drives) IAW IA directives.

1.2.11.5. Review applicable SORNs for information systems concurrently with the FISMA annual review to validate if changes to the SORN are needed.

1.2.11.6. Review IT systems registered in the Enterprise Information Technology Data Repository (EITDR); address and update responses to privacy questions in

EITDR. Failure to do so may risk system non-concurrence by the AF Privacy Officer during annual compliance review, certification, decertification, or request for funding.

1.2.12. Individuals whose jobs require routine work with and/or access to records containing PII, *shall*:

1.2.12.1. In addition to Privacy Act Annual Refresher training, complete specialized Privacy Act training annually to comply with paragraph 11.1.2.2 of this Instruction.

1.2.12.2. Immediately report any suspected or confirmed breaches of PII discovered to the United States Computer Emergency Response Team (USCERT) within one hour and to the local Privacy Manager/Monitor (see Chapter 9).

1.3. Personally Identifiable Information (PII).

1.3.1. Sensitive PII is personal information, which if lost, compromised or disclosed without authorization, could result in substantial harm, embarrassment, inconvenience, or unfairness to an individual. Some categories of PII, when maintained by the Department of Air Force, are sensitive as stand-alone data elements. Examples of such sensitive PII include:

1.3.1.1. Social Security Number (SSN) in any form.

1.3.1.2. Alien registration number (A-number).

1.3.1.3. Biometric identifier.

1.3.1.4. Financial account numbers.

1.3.2. The following information is sensitive PII when grouped with the person's name or other unique identifiers, such as address or phone number:

1.3.2.1. Driver's license number.

1.3.2.2. Medical Information.

1.3.2.3. Citizenship or immigration status.

1.3.2.4. Passport number.

1.3.2.5. Full date of birth.

1.3.2.6. Authentication information such as mother's maiden name or phone passwords.

1.3.3. PII accessed or handled by contractors. Contractors who are required to access or handle PII on behalf of the Air Force, must follow this Instruction. Organizations who have contractors accessing and handling PII must coordinate with contracting officials to ensure the contract contains the proper Privacy Act clauses: 52.224-1, *Privacy Act Notification*; and 52.224-2, *Privacy Act* as required by the *Federal Acquisition Regulation* (FAR) (see FAR website at: http://www.acquisition.gov/far/).

1.3.3.1. Contracts must be reviewed annually by the Contracting Officer Representative (COR) to ensure compliance with this Instruction.

1.3.3.2. Disclosure of PII to contractors for use in the performance of an Air Force contract is considered an official use disclosure within the agency under exception (b)(1) of the Privacy Act.

1.4. Privacy Complaints and Violations.

1.4.1. A privacy complaint is an allegation that an agency did not comply with specific provisions of the Privacy Act of 1974, as amended with respect to the maintenance, amendment, or dissemination of a SOR. A privacy violation is when an agency or individual knowingly or willfully does not comply with provisions of the Privacy Act. Privacy complaints or allegations of Privacy Act violations are not the same as PII breaches. For PII breach reporting procedures, see Chapter 9.

1.4.1.1. Privacy complaints/violations must be submitted in written form.

1.4.1.2. Alleged complaints of Privacy Act violations are processed through the supporting Privacy Manager. The Privacy Manager directs the process and provides guidance to the SOR manager. Issues that cannot be resolved at the local level shall be elevated to the HAF/MAJCOM/FOA/DRU Privacy Manager, as appropriate.

1.4.1.3. The local SOR manager shall:

1.4.1.4. Conduct an inquiry to determine if a formal investigation of the complaint or allegation of a Privacy Act violation is warranted.

1.4.1.5. Ensure a response is sent to the complainant through the Privacy Officer.

1.4.2. For Privacy Act complaints filed in a U.S. District Court against the AF, an AF activity, or an AF employee, the Office of The Judge Advocate's General Litigation Division (AFLOA/JACL) shall provide SAF/A6P a litigation summary in accordance with the format in Appendix 8 of DoD 5400.11-R, *Department of Defense Privacy Program*. When the court renders a formal opinion or judgment, AFLOA/JACL will send SAF/A6P a copy of the judgment and opinion.

1.4.3. Penalties for Violation. An individual may file a civil law suit against the Air Force for failing to comply with the Privacy Act. In addition to specific remedial actions, civil remedies include payment of damages, court costs, and attorney fees in some cases. Misdemeanor criminal charges and a fine of up to $5,000 may be imposed if:

1.4.3.1. An employee maintains a SOR without publishing the required SORN in the Federal Register or discloses Privacy Act information from a SOR, knowing that dissemination is prohibited, to anyone not entitled to receive the information.

1.4.3.2. An individual requests or obtains access to Privacy Act information on another individual under false pretenses.

1.4.4. Privacy Managers will submit reports quarterly; complaints will be categorized as follows:

1.4.4.1. Process and Procedural: For actions concerning consent, collection, and appropriate notice.

1.4.4.2. Redress: Non-Privacy Act inquiries seeking resolution of difficulties or concerns about Privacy matters.

1.4.4.3. Operational: Inquiries regarding Privacy Act matters not including Privacy Act requests for access and/or correction.

1.4.4.4. Referrals: Complaints received but referred to another office with jurisdiction over the complaint.

Chapter 2

COLLECTING PERSONAL INFORMATION FROM INDIVIDUALS

2.1. Each agency that maintains a SOR shall:

2.1.1. Only maintain in its records information about an individual that is relevant and necessary to accomplish a purpose of the agency as required by a statute or executive order or their implementing regulations.

2.1.2. Collect information to the greatest extent practicable directly from the subject individual when the information may result in adverse determinations about an individual's rights, benefits, and privileges under Federal programs.

2.1.2.1. Examples of when it is more practicable to collect information from a third party about another individual, instead of the subject individual, include but are not limited to:

2.1.2.2. Verification of information through third-party sources for security or employment suitability determinations.

2.1.2.3. Seeking third-party opinions such as supervisor comments as to job knowledge, duty performance, or other opinion-type evaluations.

2.1.2.4. Obtaining information first from the individual may impede rather than advance an investigative inquiry into the actions of the individual.

2.1.2.5. Contacting a third party at the request of the individual to furnish certain information, such as exact periods of employment, termination dates, copies of records, or similar information.

2.1.2.6. Collecting information on minor children.

2.1.3. Ensure specialized training is conducted for individuals who handle privacy information on a daily or routine basis in addition to Privacy Act Annual Refresher training.

2.1.4. Implement and enforce safeguards to ensure protection of PII.

2.1.5. Ensure required Privacy Act Notifications are provided to individuals when PII is collected.

2.2. Privacy Notifications and Safeguards.

2.2.1. Whenever an individual is requested to provided information; Inform individual of the authority, purpose, routine use, if disclosure of the information is voluntary or not, and if applicable the SORN which may apply.

2.2.1.1. Authority: The legal authority that authorizes the solicitation of the information and whether the disclosure of such information is mandatory or voluntary.

2.2.1.2. Purpose: the principal purpose or purposes for which the information is intended to be used.

2.2.1.3. Routine Uses: Who will have access to the information outside the DoD.

2.2.1.4. Disclosure: Voluntary or Mandatory. (Use mandatory only when disclosure is required by law and the individual will be penalized for not providing information. All

mandatory disclosure requirements contained in a PAS must have first been reviewed by the servicing legal office). Include any consequences of nondisclosure in nonthreatening language.

2.2.1.5. The applicable SORN(s) [*number and title*] is available at: **http://dpclo.defense.gov/privacy/SORNs/SORNs.html**.

2.2.2. Privacy Act Advisory Statements in Publications. Include a Privacy Act Advisory Statement in each Air Force publication that requires collecting or keeping personal information in a SOR. Also include a statement when publications direct collection from the individual of any part or form of the SSN. The statement shall refer to the legal authority for collecting the information and SORN number and title as follows: "This publication requires the collection and or maintenance of information protected by the Privacy Act of 1974 authorized by [set forth the legal authority such as the federal statute, executive order, and regulation]. The applicable SORN(s) [*number and title*] is available at: **http://dpclo.defense.gov/privacy/SORNs/SORNs.html**."

2.2.3. Paper or electronic documents and/or materials that contain personal information protected under the Privacy Act such as recall rosters, personnel rosters, lists or spreadsheets shall be marked in the header or top "FOR OFFICIAL USE ONLY" (IAW DoDM 5200.01, Volume 4, *DoD Information Security Program: Controlled Unclassified Information)* and with the following banner in the footer or bottom:

2.2.3.1. "The information herein is For Official Use Only (FOUO) which must be protected under the Freedom of Information Act of 1966 and Privacy Act of 1974, as amended. Unauthorized disclosure or misuse of this PERSONAL INFORMATION may result in criminal and/or civil penalties."

2.2.3.2. Paper documents and printed materials that contain PII shall be covered with the AF Form 3227, *Privacy Act Cover Sheet* or DD Form 2923, *Privacy Act Data Cover Sheet* (see paragraph 9.4.3) when removed from a SOR.

2.2.4. The Privacy Act requires agencies to provide safeguards to ensure the security and confidentiality of SOR and to protect individuals against an invasion of personal privacy. Refer to AFI 33-129, *Web Management and Internet Use*, for the appropriate procedures required to send Privacy Act information across the Internet.

2.2.4.1. Exercise caution before transmitting personal information via e-mail to ensure the message is adequately safeguarded. Some information may be so sensitive and personal that e-mail may not be the proper way to transmit it. When transmitting personal information via e-mail within DoD, ensure:

2.2.4.2. E-mail is encrypted, and

2.2.4.3. There is an official need for the recipient(s), to include those in the "cc" block, to receive the information.

2.2.5. When transmitting personal information over e-mail, encrypt and add "For Official Use Only" ("FOUO") to the beginning of the subject line and apply the following statement at the beginning of the e-mail: "This e-mail contains FOR OFFICIAL USE ONLY (FOUO) information which must be protected under the Freedom of Information Act (5 U.S.C 552) and/or the Privacy Act of 1974 (5 U.S.C. 552a). Unauthorized disclosure or misuse of this

PERSONAL INFORMATION may result in disciplinary action, criminal and/or civil penalties. Further distribution is prohibited without the approval of the author of this message unless the recipient has a need to know in the performance of official duties. If you have received this message in error, please notify the sender and delete all copies of this message." Do not indiscriminately apply this statement to all e-mails. Use it only in situations when you are actually transmitting personal information required to be protected For Official Use Only purposes. See DoDM 5200.01, Volume 4. **Note:** The guidance in this paragraph does not apply to appropriate releases of personal information to members of the public via e-mail, such as pursuant to the Freedom of Information Act, or with the consent of the subject of the personal information.

2.2.6. Do not send unencrypted e-mails containing Privacy Act information to distribution or group or non .mil e-mail addresses. Official e-mail containing Privacy Act protected information shall be digitally signed and encrypted. Before forwarding an e-mail you have received containing personal information, verify that your intended recipients are authorized to receive the information under The Privacy Act.

2.3. Social Security Number (SSN) Reduction Plan. The stated intention of the Social Security Reduction Plan is to reduce or eliminate the use of SSN in DoD and AF systems of records, IT systems and forms IAW DoDI 1000.30, *Reduction of Social Security Number (SSN) Use Within DoD*. The Functional office that owns the record for which SSNs are required to be collected is the Office of Primary Responsibility (OPR) for submitting a SSN Justification memorandum with respect to the collection of SSNs for those records. Records Professional, Privacy Manager, and Forms Manager will assist to ensure compliance with the SSN reduction plan requirements. The use of the SSN shall be limited to transactions that specifically require the presentation of the SSN to meet a statutory or regulatory requirement. Most applications that require the SSN for specific transactions do not require its use for every transaction. For example, systems that link to financial institutions may need the SSN for initial interactions, but thereafter use an account number or some other form of identification or authentication. As such there is no need to use the SSN for individuals to authenticate themselves as part of every transaction. DoDI 1000.30 is in effect and establishes.

2.3.1. Acceptable Uses: Use of the SSN includes *the SSN in any form, including, but not limited to truncated, masked, partially masked, encrypted, or disguised SSN*. The acceptable uses of the SSN are those that are provided for by law, require interoperability with organizations beyond the DoD, or are required by operational necessities. Such operational necessities may be the result of the inability to alter systems, processes, or forms due to cost or unacceptable levels of risk. Those systems, processes, or forms that claim "operational necessity" shall be closely scrutinized. Ease of use and unwillingness to change are not acceptable justifications for continuing to collect SSNs.

2.3.2. Documenting Acceptable Uses of SSN and other PII specifically. The authorization for use of PII is governed through DoD 5400.11-R. The method by which SSN use is documented shall be consistent with existing Privacy Act program requirements for forms, processes, IT systems, and systems of records, to include any locally created applications.

2.3.2.1. In addition to the documentation required for the use of PII in the PIA and/or SORN, the use of the SSN in any form as part of any collection, transfer, or retention, including locally created user applications, must be specifically documented and justified.

Documentation of the SSN justification shall be retained and available upon request. This documentation shall include:

2.3.2.1.1. The specific requirement for use of the SSN.

2.3.2.1.2. A senior official (flag officer or SES equivalent) shall sign a memorandum stating the justification for use of the SSN. It is unacceptable to collect, retain, use or transfer SSN without an approved justification.

2.3.2.1.2.1. The justification memo to collect SSN in an IT System shall be forwarded with the PIA and/or SORN to the AF Privacy Officer. The justification memo will be addressed to Defense Privacy Officer for approval/disapproval. (See Attachment 6).

2.3.2.1.2.2. Forms that collect SSN must have a completed AF Form 673 and a justification memo (IAW paragraph 2.3.2.1.2.1) that is addressed to and approved by DPCLO. Submit items to appropriate Forms Manager IAW AFI 33-360, *Publications and Forms Management*.

2.3.2.1.3. The DPCLO reviews SSN justifications for IT systems as an adjunct to the biennial PII review process. When justification for SSN use is rejected, the action officer will prepare a plan, to include milestones and a timeline, for the elimination of SSN usage.

2.3.3. Periodic Review of SSN Use and Justification. SSN use and justification memo review is a responsibility under the biennial review process for all forms. IT systems Justification memos shall be reviewed in conjunction with the FISMA Annual review.

2.3.4. Requesting the Social Security Number (SSN). When requesting an individual's SSN always give a Privacy Act Statement or Privacy Advisory, as applicable.

2.3.5. The Air Force requests an individual's SSN and provides the Privacy Act Statement/Advisory required by law when anyone enters military service or becomes an Air Force civilian employee. Confirmation of Employment Eligibility is an acceptable use. When Air Force service members or employees are asked to provide their SSN as routine identification in order to retrieve an official record, such as a medical record; it is not necessary to inform the person again why their SSN is being requested.

2.3.5.1. Alternative Means of Identifying Records: When law, executive order, or regulation does not require disclosing the SSN or if the SOR was created after January 1, 1975, a SSN may be requested, but the individual is not required to disclose it. If the individual refuses to provide their information, use alternative means of identifying records. Executive Order (E.O.) 9397, *Numbering System for Federal Accounts Relating to Individual Persons*, November 22, 1943, was amended by E.O. 13478, *Amendments to Executive Order 9397 Relating to Federal Agency Use of Social Security Numbers*, November 18, 2008, which emphasizes the need to protect PII and deletes the mandatory requirement to collecting SSNs. E.O. 9397 (SSN), as amended (E.O. 13478) shall be referenced when cited in PAS, PIA and SORN whenever a SSN is collected, used, stored, or disseminated for acceptable uses within AF IT systems, on AF Forms, or in other physical media systems of records. IT systems, AF Forms, and AF records OPRs should

also consult DoDI 1000.30, enclosure 2, paragraph 2, Acceptable Uses. Contact the OPR's organizational Privacy Office for assistance.

2.3.5.2. Protection of SSN. SSNs are personal and unique to each individual. *The SSN in any form, including, but not limited to truncated (last 4 or 5), masked, partially masked, encrypted, or disguised SSN will be Protected as High Impact PII and marked* FOR OFFICIAL USE ONLY (FOUO). Within DoD, do not disclose a person's SSN to another person without an official need to know or consent of the individual. Release of SSNs outside of the DoD are not releasable without the person's consent or unless authorized under one of the twelve exceptions to the Privacy Act (see paragraph 10.4).

2.3.6. Reporting Results of Social Security Number Reduction.

2.3.6.1. New Departmental Forms. The AF Departmental Forms Management Officer shall maintain a database to produce an annual report every July 1st. This report shall be an input into the Privacy Act section of the annual FISMA Report as required by subchapter III, chapter 35 of title 44, United States Code. The annual report shall contain the following elements:

2.3.6.1.1. Number of forms reviewed.

2.3.6.1.2. Number of forms requesting SSNs.

2.3.6.1.3. Number of SSN justifications accepted and rejected.

2.3.6.1.4. Examples of forms where SSNs were not allowed.

2.3.6.1.5. Examples of SSN masking or truncation.

2.3.6.2. For new forms issued below the departmental level (HAF/MAJCOM/FOA/DRU, Wing, etc), no database shall be required as set forth in paragraph 2.3.6.1.

2.3.6.3. Existing Departmental Forms. The AF Departmental Forms Management Officer shall report annually on July 1st the results of the AF Forms reviews and submit a report to the AF Privacy Officer. This report shall include the following elements:

2.3.6.3.1. Total number of forms in the database.

2.3.6.3.2. Number of forms reviewed.

2.3.6.3.3. Number of forms containing SSNs.

2.3.6.3.4. Number of forms where justifications were questioned.

2.3.6.3.5. Number of SSN justifications accepted and rejected.

2.3.6.3.6. Examples of forms where SSNs were not allowed.

2.3.6.3.7. Examples of SSN masking or truncation.

2.3.6.4. For existing forms issued below departmental level (HAF/MAJCOM/FOA/DRU, Wing, etc.), no reports are required at command and or base levels, with the exception of sharing best practices of specific examples where SSNs were eliminated or better masked, or for metrics collection at the AF level.

Chapter 3

FIRST PARTY ACCESS TO OWN RECORDS UNDER THE PRIVACY ACT

3.1. Making a Request for Access. Persons or their designated representatives may ask for a copy of their records maintained in a SOR. Requesters need not state why they want access to their records. Verify the identity of the requester to avoid unauthorized disclosures. How you verify identity will depend on the sensitivity of the requested records. Identity can be verified in a number of ways, to include visually, personal knowledge of the requester, a signed letter or request via telephone or e-mail, a notarized statement, or an unsworn statement. An unsworn declaration or notarized statement should be obtained in the following format:

3.1.1. "I declare under penalty of perjury (if outside the United States, add "under the laws of the United States of America") that the foregoing is true and correct. Executed on (date) (Signature)."

3.2. Processing a Request for Access. Immediately consult the local Privacy Manager, if necessary, to assure timely response to the request. When individuals request information about themselves, they are not required to site either the Privacy or Freedom of Information Act (FIOA), individual who processes the request will apply the Privacy Act when records are contained in a SOR and will apply the FOIA to all other records.

3.2.1. Requesters must adequately describe the records they want. They do not have to name a SOR, but they should at least name a type of record or functional area. For requests that ask for "all records about me," the requester should be asked for more information and tell the person how to review the government-wide systems of records published in the *Federal Register* or at **http://dpclo.defense.gov/privacy/SORNs/SORNs.html**.

3.2.2. Requesters will not use government equipment, supplies, stationery, postage, telephones, or official mail channels for making non-official requests for SOR. However, system managers shall process such requests and should advise requesters that using government resources to make non-official requests for SOR is not permissible.

3.2.3. The requester will receive an acknowledgement letter within 10 workdays, informing them of the status of their request and providing an approximate completion date of no more than 20 workdays from the date of the initial receipt of the request.

3.2.4. Show or give a copy of the record to the requester within 20 workdays of receiving the request unless the system has an exemption published in the *Federal Register* as a final rule. Give information in a form the requester can understand. If the system is exempt from disclosure under the Privacy Act, follow the procedures addressed in paragraph **3.5**.

3.3. Fees. Provide the first 100 pages free, and charge only reproduction costs for the remainder. Copies cost $.15 per page; microfiche costs $.25 per fiche. No charge for copies is made if records are provided electronically to the requester.

3.4. Do not charge fees:

3.4.1. For official purposes, such as to respond to the proposed denial of a right, privilege, or benefit; disciplinary action; or if the requester can get the record without charge under

procedures governed by DoD or AF regulation applicable to the record (for example medical records).

3.4.2. For the time to search for a Privacy Act record of the subject.

3.4.3. For reproducing a document for the convenience of the Air Force.

3.4.4. For reproducing a record so the requester can review it.

3.4.5. Fee waivers. Waive fees automatically if the direct cost of reproduction is less than $30, unless the individual is seeking an obvious extension or duplication of a previous request for which he or she was granted a waiver. Decisions to waive or reduce fees that exceed $30 are made on a case-by-case basis.

3.5. Denying or Limiting Access. When a Privacy Act system of record will not be released under the Privacy Act, the request must be processed under the FOIA. If any part of the record is denied under the FOIA, the procedures in DoD 5400.7-R_AFMAN 33-302, *DoD Freedom of Information Act Program,* are followed. For Privacy Act denials not also processed under the FOIA (Note: this should be an extremely rare circumstance), send a copy of the request, the record copy, and why access has been denied (include the applicable exemption) to the denial authority through the legal office and the Privacy Office. Judge Advocate (JA) offices shall include a written legal opinion. The legal opinion shall not merely state that the decision is "legally sufficient," but shall provide factual details and an analysis of the law and applicable regulations. The Privacy Manager reviews the file, and makes a recommendation to the denial authority. The denial authority sends the requester a letter with the decision. If the denial authority grants access, release the record copy. If the denial authority refuses access, tell the requester why and explain pertinent appeal rights (see Chapter 5).

3.5.1. Before a request for access to a Privacy Act system of record from the subject is denied that was not also processed under the FOIA, ensure that:

3.5.1.1. The system has an exemption published in the *Federal Registe*r as a final rule.

3.5.1.2. The exemption covers each document. All parts of a system are not automatically exempt.

3.5.1.3. The FOIA does not require release of any part of the record.

3.5.1.4. Nonexempt parts are segregated.

3.5.2. Third Party Information in a SOR. A first party requester is *not* entitled to information that is not "about" him or her that is contained in their system of record; for example, the home address or SSN of a third party that is contained in their system of record solely for ease of identification of the third party. Servicing legal offices should be consulted prior to the release of a third party's sensitive personal information to a first party requester that is contained in the first party requester's Privacy Act record.

3.6. Denial Authorities.

3.6.1. Initial Denial Authority (IDA). IDAs for denials of SOR to the subject of the record that is not also processed under the FOIA (Note: this should be an extremely rare case) is the same as IDAs for FOIA requests. An IDA in such a case is an official who has been granted authority by the head of a DoD component to withhold records requested under the FOIA for one or more of the nine categories of records exempt from mandatory disclosure. See DoD

5400.7-R_AFMAN 33-302, *DoD Freedom of Information Act Program*. IDA's may also deny a fee category claim by a requester; deny a request for expedited processing due to demonstrated compelling need in accordance with DoD Regulation 5400.7/AFMAN 33-302; deny a request for a waiver or reduction of fees; review a fee estimate; and confirm that no records were located in response to a request.

3.6.2. Only approved IDAs will deny all or parts of records. However, if the only information withheld from an Air Force record is privacy information under the DoD policy to withhold lists of names of DoD personnel ("DoD Names Policy"), the organization/unit FOIA Managers may sign the decision memorandum to initially deny: fee category claims, requests for expedited processing, and waiver or reduction of fees. FOIA Managers determines fee estimates; and signs "no records" responses. Organizations are authorized to withhold DoD names below O7, and e-mail addresses of most DoD personnel, under the DoD Names Policy.

Chapter 4

AMENDING A PRIVACY ACT RECORD

4.1. Amendment Reasons. Individuals may ask to have their personal information in SOR amended to make them accurate, timely, relevant, and complete. System managers shall routinely correct a record if the requester can show that it is factually wrong (e.g., date of birth is wrong).

4.2. Responding to Amendment Requests.

4.2.1. The individual may request simple corrections orally. Requests for complicated and detailed corrections must be in writing to ensure clarity.

4.2.2. After verifying the identity of the requester, make the change if appropriate, notify all known recipients of the record, and inform the individual.

4.2.3. Acknowledge requests within 10 workdays of receipt. Give an expected completion date unless you complete the change within that time. Final decisions must, unless extended by the appropriate authority, take no longer than 30 workdays of receipt.

4.3. Approving or Denying a Record Amendment. The Air Force does not usually amend a record when the change is based on opinion, interpretation, or subjective official judgment. Determination not to amend such records constitutes a denial, and requesters may appeal (see Chapter 5).

4.3.1. If the system manager decides not to amend the record; send a copy of the request, the record, and the recommended denial reasons to the denial authority through the legal office and the Privacy Office. Legal offices shall include a written legal opinion. The legal opinion shall not merely state that the decision is "legally sufficient," but will provide factual details and an analysis of the law and applicable regulations. The Privacy Officer reviews the proposed denial and legal opinion and makes a recommendation to the denial authority.

4.3.2. The denial authority sends the requester a letter with the decision. If the denial authority approves the request the record is amended.

4.3.3. The requester may file a concise statement of disagreement with the SOR manager if SAF/GCA denies the request to amend the record. SAF/GCA explains the requester's rights when they issue the final appeal decision.

4.4. Contents of Privacy Act Processing Case Files. Do not keep copies of disputed records in this file. File disputed records in their appropriate series. Use the file solely for statistics and to process requests. Do not use the case files to make any kind of determination about an individual. Document the reasons for untimely responses. These files include:

4.4.1. Requests from and replies to individuals on whether a system has records about them.

4.4.2. Requests for access or amendment.

4.4.3. Approvals, denials, appeals, and final review actions.

4.4.4. Coordination actions and related papers.

Chapter 5

APPEALS

5.1. Appeal Procedures. Individuals who receive a denial to their access or amendment request may request a denial review (appeal) within 60 calendar days of the date of the denial letter. (see paragraph 3.6).

5.1.1. The denial authority promptly sends a complete appeal package to SAF/GCA. The package must include:

5.1.1.1. The original appeal letter;

5.1.1.2. The initial request;

5.1.1.3. The initial denial;

5.1.1.4. A copy of the record;

5.1.1.5. Any internal records or coordination actions relating to the denial; the denial authority's comments on the appellant's arguments and the legal reviews.

5.1.2. If the denial authority reverses an earlier denial and grants access or amendment, notify the requester immediately.

5.1.3. The system manager may include a brief summary of the reasons for not amending the record. Limit the summary to the reasons SAF/GCA gave to the individual. The summary is part of the individual's record, but it is not subject to amendment procedures.

5.1.4. AFLOA/JACL reviews the denial and provides a final recommendation to SAF/GCA. SAF/GCA provides the requester the final Air Force decision and explains judicial review rights.

5.1.5. SAF/GCA shall provide a copy of the decision letter to the HAF/MAJCOM/FOA/DRU Privacy Officer if applicable, and the originating Privacy Manager to close the case file.

5.1.6. The records will clearly show that a statement of disagreement is filed with the record or separately, if applicable.

5.1.7. The disputed part of the record must show that the requester filed a statement of disagreement.

5.1.8. Give copies of the statement of disagreement to the record's previous recipients. Inform subsequent record users about the dispute and give them a copy of the statement with the record.

Chapter 6

DISCLOSING RECORDS TO THIRD PARTIES

6.1. Disclosure Considerations.

6.1.1. Placing PII on share drives and/or SharePoint. PII contained in any record shall not be placed on share drives for access by groups of individuals unless each person of the group has an official need to know for an approved government purpose to perform their job. Add appropriate access controls to ensure access by only authorized individuals that have the need to know. Information shall be removed when no longer needed and maintained IAW approved disposition schedule.

6.1.1.1. Recall rosters shall be marked FOUO (see paragraph 2.2.4) and only provided to individuals with an official need-to-know to accomplish their official duties. Do not place a complete recall roster in a shared location allowing everyone within the organization access; unless everyone within the organization has consented to having their information accessible by everyone within the organization.

6.1.1.2. "Social Rosters" shall be marked FOUO. Social Rosters are created in order to inform spouses/significant other of events of a social nature, such as office picnics and other events to which they will be invited. A spouse or significant other's personal information shall not be collected and maintained for social roster purposes unless collected directly from or obtain a written consent from the individual it pertains to. Personnel who maintain social rosters will ensure the information is used for its intended purpose.

6.1.2. Placing PII Files in Collaborative IT Environments. AF Information System Owners (ISO) of collaborative IT environments within the USAF enterprise, i.e., Microsoft © SharePoint, Task Management Tool (TMT), Customer Relations Management (CRM), share drives, etc., shall adhere to this Instruction and Records Management policies established for particular categories of official records.

6.1.2.1. Written permission from the owner of the SOR is required before placing electronic files or records copies into a collaborative or shared environment.

6.1.2.2. The ISO shall protect, safeguard and manage SOR and records containing PII within a shared environment according to the published SORN and/or PIA of the owners' SOR from which electronic files and records copies are shared. AF SORNs are posted on the Defense Privacy Office public website **http://dpclo.defense.gov/privacy/SORNs/SORNs.html**. AF PIAs are posted on the Air Force Privacy Act public website **http://www.privacy.af.mil/pia/index.asp**.

6.1.2.3. Organizations are not required by this directive to actively search through SharePoint or share drive to attempt to find PII which does not have the required safeguard procedures. Commands may implement additional requirements for reviewing sites. If PII is discovered, where proper safeguard measures are not in place (Need to Know to perform official duties) PII breach reporting and reprimand may be appropriate as outlined in Chapter 9 of this instruction.

6.1.3. Personal Information That Requires Protection. Following are some examples of information that is normally not releasable to the public without the written consent of the subject. This list is not all-inclusive. The facts and circumstances of the request and the nature of the record will determine the appropriateness of release without consent. Withholding personal information from AF records is always subject to balancing the specific privacy interest of individuals contained in a specific record against the public interest in the information. **Note:** Since 2001 the release of names and other PII of certain DoD personnel are given more scrutiny and the interests supporting withholding of the information given more weight. See **http://www.DoD.mil/pubs/foi/dfoipo/docs/names_removal.pdf**.

6.1.3.1. Names of personnel below the grade of O-7 or civilian equivalent, unless the DoD person is a Director of an organization.

6.1.3.2. Marital status (single, divorced, widowed, separated).

6.1.3.3. Number, name, and sex of dependents.

6.1.3.4. Civilian educational degrees and major areas of study (unless the request for the information relates to the professional qualifications for Federal employment).

6.1.3.5. School and year of graduation (if not in connection with professional qualifications for Federal employment).

6.1.3.6. Home of record.

6.1.3.7. Home/mailing address and phone/mobile numbers.

6.1.3.8. Age and date of birth (year).

6.1.3.9. Present or future assignments for overseas or for routinely deployable or sensitive units.

6.1.3.10. Office, name, state, unit address and duty phone for overseas or for routinely deployable or sensitive units.

6.1.3.11. Race/ethnic origin.

6.1.3.12. Educational level (unless the request for release of the information relates to the professional qualifications for Federal employment).

6.1.3.13. Social Security Number.

6.1.3.14. DoD Identification Number.

6.2. Releasable Information. Following are examples of information normally releasable to the public without the written consent of the subject. This list is not all-inclusive and is always subject to balancing the specific privacy interest of individuals contained in a specific record against the public interest in the information. The facts and circumstances of the request and the nature of the record will determine the appropriateness of release without consent.

6.2.1. Names of Directors or personnel above the grade of O-6 or civilian equivalent.

6.2.2. Rank.

6.2.3. Grade.

6.2.4. Air Force Specialty Code.

6.2.5. Pay (base pay, special pay, and all allowances except for Basic Allowance for Housing).

6.2.6. Gross salary for civilians.

6.2.7. Past duty assignments, unless sensitive or classified.

6.2.8. Present and future approved and announced stateside assignments.

6.2.9. Position title.

6.2.10. Office, unit address, official e-mail address, and duty phone number (CONUS only).

6.2.11. Date of rank.

6.2.12. Entered on active duty date.

6.2.13. Pay date.

6.2.14. Source of commission.

6.2.15. Professional military education.

6.2.16. Promotion sequence number.

6.2.17. Military awards and decorations.

6.2.18. Duty status of active, retired, or reserve.

6.2.19. Active duty official attendance at technical, scientific, or professional meetings.

6.2.20. Official Biographies and photos of senior personnel above the rank of O-6 or civilian equivalent.

6.2.21. Date of retirement, separation.

6.3. Disclosing Information. In all cases, use the following guidelines to decide whether to release information without consent:

6.3.1. Would the subject have a reasonable expectation of privacy in the information requested?

6.3.2. Is disclosing the information in the public interest? The public interest relates to how the Air Force carries out its statutory and regulatory duties.

6.3.3. Balance the public interest against the individual's privacy interest. Do *not* consider the requester's purpose, circumstances, or proposed use.

6.4. Rules for Releasing Privacy Act Information Without Consent of the Subject. The Privacy Act prohibits disclosure of any SOR without the written consent of the individual to whom the record pertains. There are twelve exceptions to the "no disclosure without consent" rule. See **http://www.privacy.af.mil/exceptions/index.asp**.

6.5. Disclosing the Medical Records of Minors. AF personnel may disclose the medical records of minors to their parents or legal guardians in conjunction with applicable Federal laws and guidelines. The laws of each state define the age of majority. Consult with the servicing legal office and Military Treatment Facility (MTF) for guidance in regard to the age of majority in overseas locations.

6.6. Disclosure Accountings. System managers must keep an accurate record of all disclosures made from any SOR except disclosures to DoD personnel for official use or disclosures under the FOIA. System managers may use AF Form 771, *Accounting of Disclosures*. Retain disclosure accountings for 5 years after the disclosure, or for the life of the record, whichever is longer.

6.6.1. System managers shall file the Accounting of Disclosure record and give it to the subject on request, send corrected or disputed information to previous record recipients, explain any disclosures, and provide an audit trail for reviews. Include in each accounting:

6.6.1.1. Release date.

6.6.1.2. Description of information.

6.6.1.3. Reason for release.

6.6.1.4. Name and address of recipient.

6.6.2. Some exempt systems let you withhold the accounting record from the subject.

6.6.3. You may withhold information about disclosure accountings for law enforcement purposes at the law enforcement agency's request.

6.7. Computer Matching. Computer matching programs electronically compare records from two or more automated systems of the DoD, another Federal agency, or a State or Local Government. A system manager proposing a match that could result in an adverse action against a Federal employee must meet these requirements of the Privacy Act: (1) prepare a written agreement between participants; (2) secure approval of the Defense Data Integrity Board; (3) publish a matching notice in the *Federal Register* before matching begins; (4) ensure full investigation and due process; and (5) act on the information, as necessary.

6.7.1. The Privacy Act applies to matching programs that use records from: Federal personnel or payroll systems and Federal benefit programs where matching: (1) determines Federal benefit eligibility; (2) checks on compliance with benefit program requirements; (3) recovers improper payments or delinquent debts from current or former beneficiaries.

6.7.2. Matches used for statistics, pilot programs, law enforcement, tax administration, routine administration, background checks and foreign counterintelligence, and internal matching that won't cause any adverse action are exempt from Privacy Act matching requirements.

6.7.3. Any activity that expects to participate in a matching program must contact AF Privacy Officer immediately. System managers must prepare a Computer System Matching Agree notice for publication in the *Federal Register* with a Routine Use that allows disclosing the proposed system notice to AF Privacy Officer. Allow 180 days for processing requests for a new matching program.

6.7.4. The subject of a SOR must receive a PAS when personal information of the subjects are asked to be provided and will be used in a matching program as a routine use. The most appropriate method of doing so is to include the PAS on the form used to apply for benefits. Coordinate appropriate statements with the MAJCOM/FOA/DRU Privacy Manager and AF Privacy Officer.

6.8. Privacy and the Web. Do not post PII on publicly accessible DoD web sites unless authorized by law and implementing regulation and policy. Additionally, do not post PII on .mil secure web sites unless authorized by the appropriate local commander, for official purposes, and an appropriate risk assessment is performed. See AFI 33-129.

6.8.1. Add a prominent Privacy Act Advisory at web site entry points. A Privacy Act Advisory is required to be posted on the web page where the information is being solicited or through a well-marked hyperlink whenever a web site solicits PII, even when not retained by the site after login or maintained in a SOR. Notices must clearly explain when the collection of PII is voluntary and notify users how to provide consent.

6.8.2. Include a Privacy Act Statement on the web page if it collects information directly from an individual that is maintained and retrieved by his or her name or personal identifier (i.e., SSN). Only maintain such information in approved SOR that are published in the *Federal Register*. Provide a link to the AF Privacy Act policy and SORNs at **http://www.privacy.af.mil/** and **http://dpclo.defense.gov/privacy/SORNs/SORNs.html**.

Chapter 7

PRIVACY IMPACT ASSESSMENTS

7.1. Evaluating Information Systems for Privacy Act Compliance and Risk Identification. ISOs, Portfolio Managers (PfMs), PMs, and IAMs shall address Privacy Act requirements and risks to Privacy Act data in an IT system and plan the integration of privacy protections with appropriate IA controls into the development life cycle of an information system. A PIA shall be completed in accordance with DoDI 5400.16.

7.2. What is a PIA? The Privacy Impact Assessment is an analysis of how PII information is collected and handled in an IT system: (1) to ensure PII handling conforms to applicable legal, regulatory, and policy requirements regarding privacy, (2) to determine the risks and effects of collecting, maintaining and disseminating information in identifiable form in an electronic information system, and (3) to examine and evaluate protections and alternative processes for handling PII information to mitigate potential privacy risks.

7.2.1. The PIA identifies the physical, technical, and administrative controls that are needed to protect PII. Information Assurance (IA) controls are identified in DoDI 8500.2, *Information Assurance (IA) Implementation*, that mitigate specific risks that will be implemented and tested before deployment or release of the system; and whether a SORN exists, needs to be created, and/or needs to be amended. The *E-Government Act of 2002*and DoDI 5400.16 requires PIAs to be conducted before developing or procuring IT systems or projects that collect, maintain, or disseminate information in identifiable form from or about individuals as defined in DoD 5400.11-R.

7.2.2. PIAs are required to be performed, accomplished and/or updated as necessary when a system change exposes a new privacy risk for which an IA control must be identified and tested before re-deployment or re-release of the system.

7.2.3. The depth and content of the PIA should be thorough and appropriate for the nature of the information to be collected and the size and complexity of the information technology system.

7.3. When a PIA is required. PIAs are submitted 120 days from the scheduled operational and expiration date (Authorization to Operate (ATO) or Interim Authorization to Operate (IATO)) on all new and existing systems meeting the criteria when PII, other than the user table is collected, maintained, used, or disseminated in electronic form about members of the public, Federal personnel, contractors or foreign nationals employed at U.S. military facilities internationally, in order to:

7.3.1. Ensure PII handling conforms to applicable legal, regulatory, and policy requirements regarding privacy;

7.3.2. Determine the need, privacy risks, and effects of collecting, maintaining, using, and disseminating PII in electronic form; and

7.3.3. Examine and evaluate protections and alternative processes to mitigate potential privacy risks.

7.4. When a PIA is not required. A PIA is not required when: (1) PII is not being maintained, collected, store, used, and/or disseminated; other than the user table or (2) the IT system is an approved National Security System (NSS). Administrative and personnel systems that do not meet one or more of the NSS conditions are not exempt from the PIA requirement.

7.5. Who conducts the PIA? The ISO shall conduct a PIA in conjunction with the system PM, IAM and local/functional Privacy Manager.

7.5.1. Medical IT systems that are Defense Health Program (DHP) funded or in the AF line-funded portfolio and managed by AFMS assets, shall route PIAs through the AF SG-CIO office for appropriate management, signatures, and oversight.

7.5.2. All DoD Medical Department IT systems purchased with DHP funds must ONLY be reported to the DoD Information Technology Portfolio Repository (DITPR) via the component Tricare Management Activity (TMA).

7.6. Format and Digital Signatures. PIAs shall be completed on DD Form 2930, *Privacy Impact Assessment*, as an unsecured fillable PDF which requires digital signatures as follows, except for medical DHP funded systems (see paragraph 7.5.1):

7.6.1. Obtain the first three signatures before e-mail submission to AF Privacy Officer (**airforceprivacy@pentagon.af.mil**) for review and to obtain digital signatures in the final three blocks.

7.6.2. The system Program Manager.

7.6.3. The system Information Assurance Manager.

7.6.4. The Privacy Manager.

7.6.5. The Senior Information Assurance Official (SIAO) or designee.

7.6.6. The Component Privacy Officer.

7.6.7. The AF CIO.

7.7. Submitting Approved PIAs. Approved PIAs which collect PII on members of the General Public will be forwarded by the AF Privacy Officer to the Office of the Secretary of Defense, Chief Information Officer (OSD NII/CIO) as they are required for submission to OMB; otherwise maintained by the AF and published to the AF Privacy public access website **http://www.privacy.af.mil/pia/index.asp**, sections 3 and 4 of DD Form 2930 shall be redacted of information prior to publishing, i.e., vulnerabilities and risk mitigations, classified, sensitive, and non-releasable or PII contained in an assessment.

Chapter 8

PREPARING SYSTEM OF RECORDS NOTICE (SORN) FOR PUBLISHING IN THE FEDERAL REGISTER

8.1. Publishing System of Records Notices (SORNs). Records that are retrieved by PII and/or a unique identifier are subject to Privacy Act requirements and are referred to as a SOR. The AF must submit SORNs to Defense Privacy and Civil Liberties Office (DPCLO) to be published in the *Federal Register*, describing the collection of information for new, changed or deleted systems of records. When published, the public will be allowed 30 days to comment. During this 30 day review period; collection of this information is unauthorized. Collection of the information shall begin 30 days after the SORN appears in the *Federal Register* unless comments are received that would result in a contrary determination. Any collection conducted prior to or during the 30 days comment period is an illegal collection and can result in civil penalties under the *Privacy Act OF 1974 5 U.S.C. § 552a as amended, (i)(1)Criminal Penalties*.

8.2. When is a SORN required? A SORN is required when information onan individual is retrieved by name of the indivdiual; some identifying number, symbol, or other identifying particular assigned to the individual. The Privacy Act requires submission of new or significantly changed SORNs to the Office of Management and Budget (OMB) and both houses of Congress before publication in the *Federal Register*. This applies when:

8.2.1. Starting a new system. (Add).

8.2.2. Instituting significant changes to an existing system. (Alter).

8.2.3. Minor changes to an existing system. (Admin).

8.2.4. Sending out data collection forms or Instructions.

8.2.5. Issuing a request for proposal or invitation for bid to support a new system.

8.2.6. Other Systems. National Security SOR are required to have a SORN be completed. While some or many of these systems may be classified, the SORN is written in an unclassified manner describing the nature of the collection of PII. (See DoD 5400.11-R, for the use and establishment of exemptions that may apply to these systems).

8.3. Adopting Existing SORNs. A new or existing SOR may utilize (piggy back) an existing SORN published in the *Federal Register*:

8.3.1. First, research current SORNs, including those that cover systems of records government-wide and DoD-wide on the Defense Privacy Notices website at **http://dpclo.defense.gov/privacy/SORNs/SORNs.html**, and the AF Privacy Notices website at **http://dpclo.defense.gov/privacy/SORNs/component/airforce/index.html**, for one that matches well with the new SOR at all points, i.e., Category of Individuals Covered, Category of Records, Authority, Purposes, Routine Uses, Policies, etc.

8.3.2. Second, if necessary, contact the current SORN owner through the POC information on the SORN to discuss altering or amending their SORN to include the new AF SOR and POC information.

8.3.3. Provide the system owner the altered or amended SORN for their review and processing.

8.4. Updating SORNs. Examples for Adding, Altering, Amending, and Deleting a SORN are available on the AF Information Access SharePoint and the AF Privacy Website.

8.5. Submitting SORNs for Publication in the *Federal Register*. The PM must submit the proposed SORN through their MAJCOM/FOA/DRU Privacy Manager at a minimum of 120 days before the planned implementation date of a new SOR or a change to an existing SOR subject to this Instruction. The Privacy Manager shall review for accuracy and completeness and send electronically to the AF Privacy Office **airforceprivacy@pentagon.af.mil.** The AF Privacy Office shall review and forward to DPCLO for review and publishing in the *Federal Register*, as appropriate.

8.6. Requirement for Periodic review of published SORNs. System PMs shall annually review to validate currency of their published SORNs coinciding with annual FISMA reviews and submit any changes through the process described in this chapter and promptly update appropriate answers to EITDR questions.

8.7. Deletion of SORNs. If your IT system is being decommissioned or closed and has a published SORN, comply with DoD 5400.11-R, "Deletion of System of Records Notices" and submit appropriate amendment or deletion request to the AF Privacy Office **airforceprivacy@pentagon.af.mil** to be forwarded to DPCLO to have the SORN deleted from the *Federal Register*.

Chapter 9

PROTECTING AND DISPOSING OF RECORDS

9.1. Protecting Records. Protecting privacy information is the responsibility of every federal employee, military member, and contractor who handles SOR or PII contained in any AF records.

9.2. Guidance on Protecting PII. It is AF policy that all PII collected, maintained, and stored in an electronic system shall be evaluated by the ISO for impact of loss or unauthorized disclosure and protected accordingly. Ensure coordination is accomplished between IT system PMs, IAMs and Privacy Manager. (IAWAFI 33-200, *Information Assurance (IA) Management* and DoDI 5400.16).

9.2.1. Assigning PII High or Moderate Impact Security Category (SC). All electronic systems of records shall be assigned a High or Moderate PII impact security category according to the definitions established in this Instruction and Federal Information Processing Standard (FIPS) 199, *Standards for Security Categorization of Federal Information and Information Systems*. **http://csrc.nist.gov/publications/fips/fips199/FIPS-PUB-199-final.pdf**.

9.2.2. Protect PII of High or Moderate impact security category at a Confidentiality Level of Sensitive or higher as established in DoDI 8500.2, *Information Assurance (IA) Implementation.* **http://www.dtic.mil/whs/directives/corres/pdf/850002p.pdf**, unless specifically cleared for public release (e.g., the name and contact information for selected senior officials or personnel whose duties require regular contact with the public).

9.2.2.1. As early as possible in the life cycle of IT-dependent programs, information owners shall establish the mission assurance category, security classification, sensitivity, and need-to-know of the information.

9.2.2.2. Information system owners shall establish the permissible uses of information and associated mission or business rules of use, and ensure that the distinction is clear to all personnel between information that is operationally sensitive and information that can be made available to the public.

9.2.2.3. Mission assurance category establish the requirements for availability and integrity, and security classification, sensitivity, and need-to-know establish confidentiality requirements.

9.2.2.4. Enclosure 4 of DoDI 8500.2, provides detailed lists of the IA Controls necessary to achieve the baseline levels of availability, integrity, and confidentiality for mission assurance category and classification. Any Mission Assurance Category is acceptable for DoD and AF information systems processing PII.

9.2.2.5. Electronic PII records that are assigned a High Impact Category shall be protected as follows:

9.2.2.5.1. Such records *shall not be routinely* processed or stored on portable computing devices or removable electronic media without written approval of the Information Assurance Manager (IAM). Note: IAM approval is not required in order

to remove such records contained on a government laptop computer that is removed from the primary workspace in order to telecommute or travel TDY.

9.2.2.5.2. Except for compelling operational needs, any portable computing device or removable electronic media that processes or stores High Impact PII electronic records (e.g., containing SSN) shall be restricted to workplaces that minimally satisfy Physical and Environmental Controls for Confidentiality Level Sensitive as established in DoDI 8500.2 (hereinafter referred to as "protected workplaces"). **Note:** removal of government laptop computers from primary purposes for telecommuting and TDYs is considered a compelling operational need.

9.2.3. Portable Computing Devices. Any portable computing or storage device containing High Impact PII electronic records removed from protected workplaces, including those approved for routine processing, shall:

9.2.3.1. Use an AFVA 33-276, *Privacy Act Label*, to assist in identifying and protecting Privacy Act information by placing the label on the covers of removable electronic storage media and/or deployment folders. **Note:** Creation of a Privacy Act label (for example Avery©) is authorized for use on deployment folders. AF Form 3227 or DD Form 2923 shall be used whenever the folders are removed from the approved storage area.

9.2.3.2. Require certificate based authentication using a DoD or DoD-approved Public Key Infrastructure (PKI) certificate on an approved hardware token to access the device.

9.2.3.3. Implement IA Control PESL-1 (screen lock), with a specified period of inactivity not to exceed 30 minutes (15 minutes or less recommended).

9.2.3.4. PII Data at Rest on Portable Devices. Encrypt all data at rest, i.e., data that is contained on hard drives or other storage media within portable devices as well as all removable media created by or written from the device while outside a protected workplace. If a portable device is incapable of encryption, it cannot be used to store PII. Minimally, the cryptography shall be NIST-certified (i.e., FIPS 140-2 **http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf**). See DoDI 8500.2, ECCR (Encryption for Confidentiality (Data at Rest)).

9.2.3.5. Follow guidance in for transmitting PII or other sensitive information via e-mail IAW paragraph 2.2.4 of this Instruction.

9.2.4. PII and Remote Access. Only DoD authorized devices shall be used for remote access. Any remote access, whether for user or privileged system administrator functions, must conform to IA Control EBRU- 1 (Remote Access for User Functions), EBRP- 1 (Remote Access for Privileged Functions), and ECCT-1 (Enclave and Computing Environment) as established in DoDI 8500.2 and DoD Memorandum, *Department of Defense Guidance on Protecting Personally Identifiable Information (PII)*:

9.2.4.1. Shall employ certificate based authentication using a DoD or DoD-approved PKI certificate on an approved hardware token.

9.2.4.2. The remote device gaining access shall conform to IA Control PESL- 1 (screen lock), with a specified period of inactivity not to exceed 30 minutes (15 minutes or less recommended). (See DoDI 8500.2.)

9.2.4.3. The remote device gaining access shall conform to IA Control ECRC-1, Resource Control. (See DoDI 8500.2.)

9.2.4.4. Download and local/remote storage of records containing PII is prohibited unless expressly approved by the ISO.

9.3. PII Breach Reporting. Refer to OSD Memorandum (OSD 15041-07, dated 21 September 2007), *Safeguarding Against and Responding to the Breach of Personally Identifiable Information*, Appendix A, Table 1, PII Incident Reporting and Risk Assessment Model for more specific information on PII breach reporting. A PII breach is defined as "a loss of control, compromise, unauthorized disclosure, unauthorized acquisition, unauthorized access, or any similar term referring to situations where persons other than authorized users and for an other than authorized purpose have access or potential access to PII, whether physical or electronic." (See Attachment 1). Breaches must be reported to the servicing Privacy Manager by anyone discovering it.

9.3.1. The servicing Privacy Manager shall assist with the submission of a Preliminary PII Breach Report by unencrypted e-mail according to the timeline below:

9.3.1.1. PII Breach Reports shall be completed on the template provided by DPCLO located on the SAF/APPF Information Access SharePoint Site:

9.3.1.2. Use for Preliminary and Final reports.

9.3.1.3. Use Red color font for changes made.

9.3.1.4. Reports shall not include names of individuals involved or affected by the breach. Reports are forwarded by unencrypted e-mail through the MAJCOM/FOA/DRU Privacy Manager who in turn shall notify the AF Privacy Office by official unencrypted e-mail (**airforceprivacy@pentagon.af.mil**) attaching the written PII Breach Preliminary Report.

9.3.1.5. Within one hour of the discovery of the PII breach, the servicing Privacy Manager shall ensure the US Computer Emergency Readiness Team (US CERT) has been notified IAW guidance at **www.us-cert.gov**. The servicing Privacy Manager shall, through their chain of command to the Wing Command Post submit an initial Operational Report (OPREP) if the breach may have an impact on organization operation and or potential media attention.

9.3.1.6. Within 24 hours of the PII breach, the Privacy Manager shall notify the senior level individual in the chain of command of the unit where the incident occurred and simultaneously notify the MAJCOM/FOA/DRU Privacy Manager by official unencrypted e-mail attaching the written PII Breach Preliminary Report.

9.3.1.7. Within 24 hours of being notified of the PII breach the appropriate level Privacy Manager shall notify the AF Privacy Office by official unencrypted e-mail (**airforceprivacy@pentagon.af.mil**) attaching the written PII Breach Preliminary Report.

9.3.1.8. Within 48 hours of the PII breach notification the AF Privacy Officer shall notify the DoD Privacy and Civil Liberties Office by official unencrypted e-mail (**dpclo.correspondence@osd.mil**) and concurrently the Component Senior Official for Privacy (CSOP).

9.3.1.9. Until resolved, the underlying issues that led to the breach shall continue to be reported to the AF Privacy Office IAW these reporting procedures.

9.3.1.10. The servicing Privacy Manager shall send the PII Breach Final Report when resolved in the same routing as previous notifications along with a final OPREP.

9.3.2. Guidelines for conducting an inquiry of a PII Incident. The senior-level individual who is in the chain of command for the organization where the loss, theft or compromise occurred shall appoint an official to conduct an inquiry (recommend E7/above or civil equivalent) on the PII incident to determine if it is an actual breach, the cause and if a there was any criminal intent that would warrant a criminal investigation.

9.3.2.1. The servicing Privacy Manager/Monitor shall provide guidance to the individual appointed to properly complete the PII Breach Final Report and reference AFI and DoD Policies and the Privacy Act for use in completing the inquiry as required.

9.3.2.2. The appointed official shall review the initial PII Incident Preliminary Report and independently assess the handling of the breach. They shall make clarifications and additions on the PII Incident Final Report as required, and submit to the appointing senior-level individual a recommendation of whether notification to affected individuals is required after a risk assessment analysis has been completed, along with any corrective actions that should be taken. A legal review shall be completed before submission of the Final Report to determine the legal sufficiency of the report and advise whether administrative, disciplinary action or a criminal investigation is warranted and appropriate. The appointed official may be asked by the appointing senior-level individual to make additional recommendations or more formal reports as required.

9.3.2.3. Upon concurrence with PII Breach Final Report recommendations, the senior-level individual who is in the chain of command for the organization where the loss, theft or compromise occurred shall route the Final Report to the appropriate level Privacy Manager.

9.3.2.4. Notification to affected individuals, if determined to be required, are normally made no later than 10 working days after a PII breach is confirmed and the identities of the affected individuals ascertained by a senior level individual in the chain of command for the organization where the breach occurred. A senior level official is considered to be at a Directorate or higher level. Group or higher level commanders of the O-6 rank or above also meet the definition of "senior level." (See Attachment 7.)

9.3.3. Air Force Computer Emergency Response Team (AFCERT) Reported PII Incidents. According to CJCSM 6510.01A, Enclosure C, Paragraph 7.b, "when a Computer Network Defense Service Provider (CNDSP) discovers compromised or potentially compromised PII, they must notify the US CERT and their Service Privacy Office POC."

9.3.3.1. AFCERT shall follow through on CNDSP detections of PII Incidents by notifying the ISO and PM of the web application and/or IT system cited.

9.3.3.2. ISO and PM of web application and/or IT system responsible for the PII breach must notify the servicing Privacy Manager/Monitor who shall ensure PII Breach notifications are accomplished as established by AF policy and DoD reporting guidance.

9.4. Risk Based Management. Apply a risk based management approach. Evaluate the effectiveness of additional protections against sensitivity, probability of exposure, risk and cost.

9.4.1. Consider the sensitivity category (Low, Moderate, or High) of the PII and the probability of exposure, risk of disclosure, loss or alteration, when providing physical security measures. (See Attachment 5.)

9.4.2. Information marked For Official Use Only (FOUO) or Controlled Unclassified Information (CUI) must be protected from unauthorized disclosure. Reasonable steps shall be taken both during and after working hours to minimize risk of access by unauthorized personnel. Guidance on marking and physical security requirements for CUI and FOUO are addressed in AFI 31-401, *Information Security Program Management* and DoDM 5200.01, Volume 4.

9.4.3. AF Form 3227, *Privacy Act Cover Sheet* or DD Form 2923, *Privacy Act Data Cover Sheet*. Use is mandatory to protect PII from being viewed by unauthorized personnel when Privacy Act materials are removed from their system of record or approved storage location.

9.4.4. AFVA 33-276, *Privacy Act Label*. Use is mandatory to assist in identifying Privacy Act information by placing the label on the covers of removable electronic storage media such as Laptops, Government Hard drives, DVDs, CDs, diskettes, tapes and/or deployment folders. The label is not authorized for use on file drawers or file folders, cabinets, or other stationary equipment or materials IAW with AFI 33-322, *Air Force Records Management.*

9.5. Disposing of Records. Consult a Records Professional before disposing of any records. You may use the following methods to dispose of records protected by the Privacy Act for authorized destruction according to RDS maintained in the Air Force Records Information Management System (AFRIMS).

9.5.1. Destroy by any reasonable method that prevents loss, theft or compromise during and after destruction such as pulping, macerating, tearing, burning, shredding or otherwise completely destroying the media so that PII is both not readable and is beyond reconstruction. Refer to NIST SP800-88, **http://csrc.nist.gov/publications/nistpubs/800-88/NISTSP800-88_rev1.pdf** .

9.5.2. Degauss or overwrite magnetic media according to established guidelines. DoDM 5200.01, Volume 4 and AFI 31-401 also govern destruction of FOUO and CUI.

9.5.3. Recycling of material protected under the Privacy Act.

9.5.3.1. When safeguarding information protected under the Privacy Act can be assured as described in this chapter, disposal of recyclable Privacy Act protected products may be accomplished through the Defense Reutilization and Marketing Office (DRMO) or through contracted recycling providers that manage a base-wide recycling program.

9.5.3.2. Originators of material protected under the Privacy Act must safeguard it until it is transferred to the recycling provider. This transfer does not require a disclosure accounting. Note: Information protected under the Privacy Act shall not be placed in unattended recycle or trash bins.

Chapter 10

PRIVACY ACT EXEMPTIONS

10.1. Exemption Types. This chapter contains the most current exemptions that have been published as final rules for the listed systems of records as of the date of this AFI. The ISO should ensure that a more recent final rule has not been published. There are two types of exemptions from release or disclosure permitted by Title 5, USC 552a:

10.1.1. *A General exemption* authorizes the exemption of a SOR from most parts of the Privacy Act.

10.1.2. *A Specific exemption* authorizes the exemption of a SOR from only a few parts of the Privacy Act.

10.2. Authorizing Exemptions. Denial authorities may withhold release or disclosure of records to the first party requesters using Privacy Act exemptions *only* when an exemption for the SOR has been published in the *Federal Register* as a final rule. See **http://dpclo.defense.gov/privacy/SORNs/component/airforce/index.html**; exemptions are noted in the right column.

10.3. Requesting an Exemption. An ISO who believes that a system requires an exemption from some or all of the requirements of the Privacy Act shall send a request through the Wing Privacy Office, the HAF/MAJCOM/FOA/DRU Privacy Office, and to AF Privacy Office. Final approval is by DPCLO. The request will detail the reasons why the exemption applies, the section of the Act that allows the exemption, and the specific subsections of the Privacy Act from which the system is to be exempted, with justification for each subsection.

10.4. Exemptions. Exemptions permissible under Title 5 are located at **http://uscode.house.gov/search/criteria.shtml**:

10.4.1. The (j) (2) exemption. Applies to investigative records created and maintained by law-enforcement activities whose principal function is criminal law enforcement.

10.4.2. The (k) (1) exemption. Applies to information specifically authorized to be classified according to DoDM 5200.01, Volume 4.

10.4.3. The (k) (2) exemption. Applies to investigatory information compiled for law-enforcement purposes by non-law enforcement activities and which is not within the scope of the (j) (2) exemption. However, the AF must allow an individual access to any record that is used to deny rights, privileges or benefits to which he or she would otherwise be entitled by Federal law or for which he or she would otherwise be eligible as a result of the maintenance of the information (unless doing so would reveal a confidential source).

10.4.4. The (k) (3) exemption. Applies to records maintained in connection with providing protective services to the President and other individuals under Title 18; Crimes and Criminal Procedure, USC, section 3056; Powers, authorities, and duties of United States Secret Service.

10.4.5. The (k) (4) exemption. Applies to records maintained solely for statistical research or program evaluation purposes and which are not used to make decisions on the rights, benefits, or entitlement of an individual except for census records which may be disclosed

under Title 13, CENSUS, U.S.C., Section 8; Authenticated transcripts or copies of certain returns; other data; restriction on use; disposition of fees received.

10.4.6. The (k) (5) exemption. Applies to investigatory material compiled solely for the purpose of determining suitability, eligibility, or qualifications for U.S. civilian employment, military service, U.S. contracts, or access to classified information, but only to the extent such material would reveal the identity of a confidential source. This provision allows protection of confidential sources used in background investigations, employment inquiries, and similar inquiries that are for personnel screening to determine suitability, eligibility, or qualifications.

10.4.7. The (k) (6) exemption. Applies to testing or examination material used solely to determine individual qualifications for appointment or promotion in the U.S. or military service, if the disclosure would compromise the objectivity or fairness of the test or examination process.

10.4.8. The (k) (7) exemption. Applies to evaluation material used to determine potential for promotion in the Military Services, but only to the extent that the disclosure of such material would reveal the identity of a confidential source.

Chapter 11

PRIVACY ACT TRAINING

11.1. Who Needs Training. The Privacy Act requires that all DoD and pertinent contractor personnel involved in the design, development, operation and maintenance of any SOR be trained annually in the principles and requirements of the Privacy Act; personnel who may be expected to deal with the news media or the public, as well as personnel specialists, finance officers, knowledge operations managers, supervisors, and individuals working with medical, personnel, financial, and security records. Privacy Act annual refresher training is also required. Training shall include rules of behavior and consequences when rules are not followed. Emphasis shall be made of the penalties and fines related to violations of the Privacy Act. Additional or advanced training should be provided commensurate with increased responsibilities or change in duties.

11.1.1. Commanders/Directors shall ensure training and communication related to privacy and security is job specific and commensurate with an individual's responsibilities. Such training shall be a prerequisite before an employee, military member, or contractor is permitted to access DoD information systems that contain Privacy Act material. Such training is mandatory for AF military personnel, employees and managers, and shall include contractors and business partners. Training must be provided and documented by the Privacy Manager/Monitor. (see Attachment 8 for DoD approved training websites).

11.1.2. Commanders shall ensure their personnel receive the following Privacy training:

11.1.2.1. Orientation Training. Training that provides individuals with a basic understanding of the requirements of the Privacy Act as it applies to the individual's job responsibilities. The training shall be provided to all personnel and as a prerequisite to all other levels of Privacy training.

11.1.2.2. Specialized Training. Training that provides information as to the application of specific provisions of this Instruction to specialized areas of job performance. Personnel of particular concern include, but are not limited to personnel specialists, finance officers, special investigators, knowledge operations managers, public affairs officials, IT professionals, and any other personnel responsible for implementing or carrying out functions under this Instruction.

11.1.2.3. Management Training. Training that provides managers and decision makers considerations that they should take into account when making management decisions regarding actions under the Privacy Program.

11.1.2.4. SOR Training. Ensure individuals who work with a SOR are trained on the provisions of the SOR notice and this Instruction. Stress individual responsibilities and advise individuals of their rights and responsibilities under this Instruction and penalties under the Privacy Act.

11.1.2.5. Annual Refresher Training. Provide annual refresher training to ensure employees and managers, as well as contractor personnel, continue to understand their Privacy Act responsibilities. U.S. personnel with authorized access to PII shall annually complete refresher training prior to granting access. An annual training certificate shall

be provided at the completion of annual refresher training online. Retain certificates in either the AF centralized electronic training record, personnel record, or in the training manager office to which the employee is assigned. When contractor personnel are involved, retain certificates in the training office of the appropriate AF activity supported by the contract.

11.2. Privacy Act Training Tools. Helpful resources include:

11.2.1. The Privacy Act web page includes a Privacy Overview, Privacy Act training slides, the Air Force SORNs, and links to the Defense Privacy Board Advisory Opinions, the DoD and Department of Justice Privacy web pages. Go to **http://www.privacy.af.mil/index.asp**. Click on "Resources" and "Training." **http://www.privacy.af.mil/training/index.asp**.

11.2.2. "*The Privacy Act of 1974*," a 32-minute film developed by the Defense Privacy Office. Contact the Joint Visual Information Services Distribution Activity at DSN 795-6543 or commercial (570) 895-6543, and ask for #504432 "*The Privacy Act of 1974*."

11.2.3. A Manager's Overview, *What You Need to Know About the Privacy Act*. This overview gives you basic Privacy Act training and is available on-line at **http://www.privacy.af.mil/training/index.asp**.

11.2.4. Training slides for use by Privacy Managers/Monitors, are available in the "Information Access SharePoint Site."

11.2.5. DISA web based training service on ADLS. An authorized user on the .mil domain can go directly to ADLS **https://golearn.csd.disa.mil** "Course List" for "Total Force Awareness Training" then "Information Protection" which includes mandatory Privacy Act and Information Assurance annual refresher course and a PII course at **http://iase.disa.mil/eta/index.html#onlinetraining**.

Chapter 12

CIVIL LIBERTIES

12.1. Basic Guidelines. DODI 1000.29, *Department of Defense Civil Liberties program* requires at least one senior official designated to advise the Secretary of Air Force (SECAF) on Civil Liberties matters and to meet the following statutory requirements:

12.1.1. Assist the SECAF in appropriately considering Civil Liberties concerns when the AF is proposing, developing, or implementing laws, regulations, policies, procedures, or guidelines related to efforts to protect the Nation against terrorism;

12.1.2. Periodically investigate and review AF actions, policies, procedures, guidelines and related laws and their implementation to ensure that the AF is adequately considering Civil Liberties in its actions;

12.1.3. Ensure that the AF has adequate procedures to receive, investigate, respond to, and redress complaints from individuals who allege that the AF has violated their Civil Liberties;

12.1.4. In providing advice on proposals to retain or enhance a particular governmental power, the DoD Civil Liberties Officer shall consider whether the AF has established the following;

12.1.4.1. Whether the need for the power is balanced with the need to protect Civil Liberties;

12.1.4.2. Whether the AF provides adequate supervision to ensure that Civil Liberties are protected during the execution of the governmental power , and

12.1.4.3. Whether there are adequate guidelines and oversight to properly confine its use.

12.2. Civil Liberties. Civil liberties are fundamental rights and freedoms protected by the Constitution of the United States. These freedoms, which include the right to privacy, are concentrated primarily in the Bill of Rights. Individuals who feel any of the following provided examples (the list is not exhaustive) has been violated shall seek guidance through their servicing Inspector General (IG) office; (see AFI 90-301, *Inspector General Complaints Resolution)*.

12.2.1. First Amendment: Freedom of Religion; Freedom of Speech or of the Press; Right to Peaceably Assemble and to Petition the Government for a redress of grievances.

12.2.2. Second Amendment: Right to Keep and Bear Arms.

12.2.3. Fourth Amendment: Right Against Unreasonable Searches and Seizures.

12.2.4. Fifth Amendment: Prohibition Against Deprivation of Life, Liberties, or Property, without due process of law.

12.2.5. Fifteenth, Nineteenth and Twenty Sixth Amendments: Right to Vote.

12.3. Responsibilities.

12.3.1. The Component Senior Official for Privacy is designated as the AF Civil Liberties Officer. The AF Civil Liberties Officer shall:

12.3.1.1. Oversee the AF Civil Liberties program with execution by the AF Civil Liberties point of contact (POC).

12.3.1.2. Review and approve AF Civil Liberties reports prior to submission to DPCLO.

12.3.2. The AF Privacy Officer is designated as the AF Civil Liberties POC. The Air Force Privacy Officer shall:

12.3.2.1. Serve as the AF member on the Defense Civil Liberties board.

12.3.2.2. Provide policy and guidance for the AF Civil Liberties program.

12.3.2.3. Review AF publications and policies to support the proper protection of Civil Liberties.

12.3.2.4. Compile and submit the AF Quarterly Civil Liberties report to the AF Civil Liberties Officer for approval.

12.3.2.5. Provide Secretary of the Air Force (SAF)/General Counsel (GC) with copies of the AF Quarterly Civil Liberties report for situational awareness.

12.3.2.6. Maintain the AF Civil Liberties website to ensure POCs, training materials, and Civil Liberties guidance are current.

12.3.2.7. Provide training and training materials to MAJCOM, DRU, FOA and base Civil Liberties points of contact. Create and maintain the Annual Civil Liberties ADLS training.

12.3.3. SAF/IG and AF/A1 shall:

12.3.3.1. Coordinate with SAF/GC on any Civil Liberty matters, reviews, or investigations, that involve the following: represent a significant litigation risk; impact major AF programs; materially impact the rights or benefits of an AF organization; affect ownership or use of AF property; attract Congressional interest; attract widespread media interest; raise a matter of first impression for the legal community; or otherwise affect the legal basis for an AF program or activity.

12.3.3.2. Identify and report Civil Liberties complaint allegations received and processed by IG or EEO/ MEO offices on a quarterly basis.

12.3.3.3. Submit complaint(s) with Civil Liberties implications to the AF Civil Liberties POC using the quarterly report template. (See Attachment 11). Reports are forwarded directly by unencrypted e-mail without identifying PII to the AF Civil Liberties workflow e-mail at **afcivil.Liberties@pentagon.af.mil**.

12.3.3.4. Provide Civil Liberties reporting requirements guidance to the MAJCOMS, DRU, and FOA IG offices.

12.3.4. AF/JAA shall:

12.3.4.1. Provide legal advice on Civil Liberties matters to the AF Civil Liberties Officer and Civil Liberties POC.

12.3.4.2. Review Civil Liberties Quarterly Reports for legal sufficiency.

12.3.4.3. Provide Civil Liberties reporting requirements to HAF/MAJCOM/FOA/DRU EO offices.

12.3.5. SAF/GC shall provide coordination on any civil liberty matters, reviews, or investigations, or legal opinions that represent a significant litigation risk, impact major Air Force programs, materially impact the rights or benefits of an Air Force organization, effect ownership or use of Air Force property, engender Congressional interest, attract widespread media interest, raise a matter of first impression for the legal community, or otherwise affect the legal basis for an Air Force program or activity.

12.3.6. MAJCOM, DRU, FOA and base legal offices shall:

12.3.6.1. On a quarterly basis, identify and report Civil Liberties complaint allegations addressed in Commander Directed Investigation (CDI) reports and Article 138 complaints that have been reviewed for legal sufficiency.

12.3.6.2. Submit civil Liberties complaint contained in CDIs and Article 138 complaints to the Civil Liberties POC, through AF/JAA, using the quarterly reporting template. (See Attachment 11). Reports are forwarded by unencrypted e-mail without identifying PII.

12.3.6.3. Provide advice to the Civil Liberties POCs.

12.3.7. MAJCOM/A6s and Communication Squadron Commanders shall:

12.3.7.1. Are responsible for overall implementation of the AF Civil Liberties Program for personnel under their command/supervision.

12.3.7.2. Shall appoint a Privacy Manager to be the Civil Liberties POC for their organization, with commensurate duties and responsibilities.

12.3.8. The Civil Liberties POCs shall:

12.3.8.1. Administer guidance and procedures prescribed in this Instruction.

12.3.8.2. Conduct mandatory reviews of publications and forms created at their level to support the proper protection of Civil Liberties.

12.3.8.3. Ensure training is available for their organizations.

12.3.8.4. As needed, provide updates regarding the Civil Liberties POCs' names, office symbols, voice number, and unclassified e-mail addresses to the AF Civil Liberties POC.

12.3.8.5. Promote Civil Liberties awareness throughout their organizations.

12.3.8.6. Direct complaints that may have Civil Liberties implications to the appropriate investigative office, such as the IG, EO, or the appropriate commanding officer for commander directed investigations.

12.4. Civil Liberties Quarterly Report.

12.4.1. The AF Civil Liberties Officer will submit a quarterly report to DPCLO IAW DoDI 1000.29 (Attachment 10). Quarterly reports are on a fiscal year schedule and are due to the DoD Civil Liberties office on the 15th of January, April, July and October.

12.4.2. AF/A1, SAF/IG, and AF/JAA will submit Civil Liberties reports to SAF/A6PP on the 8th of the month following the end of the quarter in order to meet the DoD suspense date. Civil Liberties reports will not report Civil Liberties complaints in the following circumstances: during the Uniform Code of Military Justice process (Courts-Martial/Non-

Judicial Punishment); administrative discharge process, or situations whereby an Inspector General reprisal and restriction complaint may be duplicated.

12.5. Reprisal For Making Complaint: No Air Force member, employee, or contractor shall take any action constituting a reprisal, or threat of reprisal, in response to a Civil Liberties complaint or a disclosure of information to a Privacy or Civil Liberties Officer; provided, however, that disciplinary action may be taken if the Civil Liberties compliant or disclosure of information was made with the knowledge that such complaint or disclosure was false, or made with a willful disregard for its truth or falsity.

12.6. Who Needs Training. AF Personnel.

12.6.1. Annual Civil Liberties training is mandatory for AF personnel to include military, civilians, contractors, and business partners. Refresher training shall be accomplished as required.

12.6.2. Commanders shall ensure their personnel receive the following Civil Liberties training:

12.6.2.1. Management Training. Training that provides managers and decision makers considerations that they should take into account when making management decisions regarding actions under the Civil Liberties Program.

12.6.2.2. Annual Training: AF personnel shall complete the annual Civil Liberties Advance Distance Learning System (ADLS) training.

12.6.2.3. Refresher Training. After any adjudicated violation within an organization, provide refresher training to ensure employees, managers, and contractor personnel, have an adequate understanding of the Air Force Civil Liberties program.

12.7. Civil Liberties Training Tools.

12.7.1. The AF Civil Liberties web page includes an overview, and will include Civil Liberties training slides and links to other DoD training on Civil Liberties. Click on "Resources" and "Training." **http://www.privacy.af.mil/training/index.asp**.

12.7.2. "The Asylum Seekers Overview." This online training provided by the Department of Homeland Security (DHS) provides law enforcement personnel with essential information related to asylum seekers. The course serves as a resource to support the DHS's commitment to securing America while providing established protections for asylum seekers. **http://www.dhs.gov/xlibrary/assets/training/xus/crcl/asylumseekers/index.htm**.

12.7.3. The Common Muslim American Head Coverings and Common Sikh American Head Coverings Posters. These posters provide guidance to DoD personnel on the appropriate ways in which to screen and, if necessary, search Muslim or Sikh individuals wearing various types of religious head coverings.

12.7.4. "The First Three to Five Seconds." This training introduces law enforcement officers to basic principles of the Arab American and Muslim American cultures. **http://www.dhs.gov/xlibrary/assets/training/xus/crcl/three-fiveseconds/index.htm**.

MICHAEL J. BASLA, Lt Gen, USAF
Chief, Information Dominance and Chief Information Officer

Attachment 1

GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION

References

Title 5 United States Code, Section 552a, as amended, *The Privacy Act of 1974*

Title 5 United States Code Section 552, as amended, *The Freedom of Information Act of 1966*

Executive Order 9397, *Numbering System for Federal Accounts Relating to Individual Persons,* 30 November 1943

Executive Order 13478, *Amendments to Executive Order 9397 Relating to Federal Agency Use of Social Security Numbers,* 18 November 2008

Public Law 100-235, *The Computer Security Act of 1987*, 8 January 1988

Public Law 107-347, Section 208, *E-Government Act of 2002, Federal Information Security Management Act (FISMA),* 17 December 2002

Public Law 110-53, Section 803, *Privacy and Civil Liberties Officers, Implementing Recommendations of the 9/11 Commission Act of 2007*, 3 August 2007

DoDD 5400.11, *DoD Privacy Program*, 8 May 2007

DoDD 5100.3, *Support of the Headquarters of Combatant and Subordinate Unified Commands,* 9 February 2011

DoDI 1000.29, *DoD Civil Liberties Program*, 17 May 2012

DoDI 1000.30, *Reduction of Social Security Number (SSN) Use Within DoD*, 1 August 2012

DoDI 5400.16, *DoD Privacy Impact Assessment (PIA) Guidance,* 12 February 2009

DoDI 8500.2, *Information Assurance (IA) Implementation*, 6 February 2003

DoD 5200.01-M, Volume 4, *Department of Defense Information Security Program: Controlled Unclassified Information (CUI),* 24 February 2012

DoD 5400.7-R_AFMAN 33-302, *DoD Freedom of Information Act Program,* 21 October 2010

DoD 5400.11-R, *DoD Privacy Program*, 14 May 2007

DoD 6025.18-R, *DoD Health Information Privacy Regulation*, 24 January 2003

AFPD 33-3, *Information Management*, 8 September 2011

AFI 31-401, *Information Security Program Management*, 1 November 2005

AFI 33-129, *Web Management and Internet Use,* 3 February 2005

AFI 33-200, *Information Assurance (IA) Management,* 23 December 2008

AFI 33-320, *Federal Register,* 15 May 2002

AFI 33-322, *Records Management Program*, 4 June 2012

AFI 33-324, *The Information Collections and Reports Management Program: Controlling Internal, Public, and Interagency Air Force Information Collections*, 1 June 2000

AFI 33-360, *Publications and Forms Management*, 18 May 2006

AFI 41-210, *TRICARE Operations and Patient Administration Functions*, 6 June 2012

AFI 90-301, *Inspector General Complaints Resolution*, 23 August 2011

AFMAN 33-363, *Management of Records*, 1 March 2008

Air Force Records Information Management System (AFRIMS)

AFVA 33-276, *Privacy Act Label*, 1 August 2000

Federal Information Processing Standard (FIPS) 140-2, *Security Requirements For Cryptographic Modules*, 25 May 2001

Federal Information Processing Standard (FIPS) 199, *Standards for Security Categorization of Federal Information and Information Systems*, February 2004

Federal Acquisition Regulation (FAR), current edition

Prescribed Forms

AF Form 3227, *Privacy Act Cover Sheet*

Adopted Forms

DD Form 2923, *Privacy Act Data Cover Sheet*

DD Form 2930**,** *Privacy Impact Assessment*

AF Form 771, *Accounting of Disclosures*

AF Form 847, *Recommendation for Change of Publication*

Abbreviations and Acronyms

AFCERT—Air Force Computer Emergency Response Team

AF CIO—Air Force Chief Information Officer

AFBCMR—Air Force Board for Correction of Military Records

AFI—Air Force Instruction

AFLOA—Air Force Legal Operations Agency

AFMAN—Air Force Manual

AFMS—Air Force Medical Service

AFPD—Air Force Policy Directive

AFRIMS—Air Force Records Information Management System

ATO—Authorization to Operate

CIO—Chief Information Officer

CDI—Commander Directed Investigation

CFR—Code of Federal Regulations

CSOP—Component Senior Official for Privacy

CUI—Controlled Unclassified Information

DCS—Deputy Chief of Staff

DHP—Defense Health Program

DHS—Department of Homeland Security

DITPR—DoD Information Technology Portfolio Repository

DoD—Department of Defense

DPCLO—Defense Privacy and Civil Liberties Office

DRMO—Defense Reutilization and Marketing Office

DRU—Direct Reporting Unit

EITDR—Enterprise Information Technology Data Repository

EO—Equal Opportunity

FIPS—Federal Information Processing Standard

FISMA—Federal Information Security Management Act

FOA—Field Operating Agency

FOIA—Freedom of Information Act

FOUO—For Official Use Only

FRN—Federal Register Notice

GOCO—Government-Owned Contractor-Operated

GSA—General Services Administration

HAF—Headquarters Air Force

IA—Information Assurance

IAM—Information Assurance Manager

IATO—Interim Authorization to Operate

IG—Inspector General

ISO—Information System Owner

IT—Information Technology

MAJCOM—Major Command

NIST—National Institute of Standards and Technology

NSS—National Security System

OMB—Office of Management and Budget

OPR—Office of Primary Responsibility

OPREP—Operational Report

PA—Stands for Public Affairs or Privacy Act, depending on context used.

PAS—Privacy Act Statement

PIA—Privacy Impact Assessment

PII—Personally Identifiable Information

PKI—Public Key Infrastructure

PL—Public Law

PM—Program Manager

SAF—Secretary of the Air Force

SIAO—Senior Information Assurance Official

SJA—Staff Judge Advocate

SOR—System of Records

SORN—System of Records Notice

SSN—Social Security Number

US—United States

USC—United States Code

USCERT—United States Computer Emergency Response Team

WHS—Washington Headquarters Services

WWW—World Wide Web

Terms

Access—Allowing individuals to review or receive copies of government records that contain personally identifiable information about them.

Amendment—The process of adding, deleting, or changing information in a SOR to make the data accurate, relevant, timely, or complete.

Alteration—A significant increase or change in the number or type of individuals about whom records are maintained. Increases in numbers of individuals due to normal growth are not considered alterations unless they truly alter the character and purpose of the system. Increases that change significantly the scope of population covered (for example, expansion of a SOR covering a single command's enlisted personnel to include all of the Component's enlisted personnel would be considered an alteration). A reduction in the number of individuals covered is not an alteration, but only an amendment. Changes that add new categories of individuals to system coverage require a change to the "Categories of individuals covered by the system" caption of the notice and may require changes to the "Purpose(s)" caption.

Biometric—Physiological and/or behavioral characteristics that are measurable and can be used to verify the identity of an individual.

Breach—A loss of control, compromise, unauthorized disclosure, unauthorized acquisition, unauthorized access, or any similar term referring to situations where persons other than

authorized users and for an other than authorized purpose have access or potential access to PII, whether physical or electronic.

Civil Liberties—Fundamental rights and freedoms protected by the Constitution of the United States.

Computer Matching—A computerized comparison of two or more automated systems of records or a SOR with non-Federal records to establish or verify eligibility for payments under Federal benefit programs or to recover delinquent debts for these programs.

Confidentiality—An expressed and recorded promise to withhold the identity of a source or the information provided by a source.

Controlled Unclassified Information (CUI)—Types of information that require application of controls and protective measures for a variety of reasons. This information is also known as "unclassified controlled information."

Cookie—Data created by a Web server that is stored on a user's computer either temporarily for that session only or permanently on the hard disk (***persistent cookie***). It provides a way for the Web site to identify users and keep track of their preferences. It is commonly used to "maintain the state" of the session. A ***third-party cookie*** either originates on or is sent to a Web site different from the one you are currently viewing.

Defense Data Integrity Board—Composed of representatives from DoD components and services who oversee, coordinate, and approves DoD computer matching programs covered by the Act.

Denial Authority—The individuals with authority to deny requests for access or amendment of records under the Privacy Act.

Disclosure—The transfer of any personally identifiable information from a SOR by any means of communication (such as oral, written, electronic, mechanical, or actual review) to any person, private entity, or Government Agency, other than the subject of the record, the subject's designated agent, or the subject's legal guardian.

Federal Agency—A department, independent agency, commission, or establishment of the Executive Branch.

For Official Use Only (FOUO)—Is a designation that is applied to unclassified information that may be exempt from mandatory release to the public under the Freedom of Information Act (FOIA).

Federal Benefit Program—A federally funded or administered program for individuals that provides cash or in-kind assistance (payments, grants, loans, or loan guarantees).

Federal Personnel—Officers and employees of the Government of the United States, members of the uniformed services (including members of the Reserve Components), and individuals entitled to receive immediate or deferred retirement benefits under any retirement program of the United States (including survivor benefits).

First Party Requester—A subject or designated representative asking for access to his/her SOR. The identity of the subject requester must be verified. A notarized signature or a sworn declaration under penalty from the record subject is one method to determine identification.

Individual— Under the Privacy Act, a citizen of the United States or an alien lawfully admitted for permanent residence.

Member of the Public—Any individual or party acting in a private capacity to include Federal employees or military personnel.

Minor—Anyone under the age of majority as an adult according to local state law. The legal age of majority may be different in overseas locations. If there is no applicable state law, a minor is anyone under the age of 18 years. Military members and married persons are not minors, no matter what their chronological age.

PII—Personally Identifiable Information; see *Personal Identifier* and *Personal Information*.

Personal Identifier—A name, number, or symbol that is unique to an individual and can be used to trace an individual identity, usually the person's name or SSN.

Personal Information— Information about an individual that identifies, links, relates, or is unique to, or describes him or her, e.g., SSN; age; military rank; civilian grade; marital status; race; salary; home/office phone numbers; other demographic, biometric, personnel, medical, and financial information, etc. Such information is also known as *personally identifiable information* (PII) (i.e., information which can be used to distinguish or trace an individual's identity, such as their name, social security number, date of birth, place of birth, mother's maiden name, or biometric records, including any other PII which is linked or linkable to a specified individual).

Privacy Act Request—A request from an individual for notification as to the existence of, access to, or amendment of records pertaining to that individual. These records must be maintained in a SOR.

Privacy Act Statement—A statement required when soliciting personally-identifying information that is maintained in a SOR. The Privacy Act Statement informs the individual why the information is being solicited and how it will be used.

Privacy Act System Notice—See System of Records Notice (SORN).

Privacy Act System of Records— See SOR

Privacy Act Complaint—An allegation that the Agency did not comply with specific provisions of the Privacy Act, 5 USC section 552a, with respect to the maintenance, amendment, or dissemination of SOR.

Privacy Act Violations—When an individual or agency who knowingly and/or willingly makes a determination under the Privacy Act of 1974 paragraph (d)(3) not to amend.

a. When an individual or agency who knowingly and/or willingly makes a determination under the Privacy Act of 1974 paragraph (d)(3) not to amend an individual's records in accordance with his/her request, or fails to make such review in conformity with that subsection; refuses to comply with an individual request under (d)(1); fails to maintain any records concerning: any individual with such accuracy, relevance, timeliness, and completeness as is necessary to assure fairness in any determination to the qualifications, character, rights, or opportunities of, or benefits to the individual that may be made on the basis of such record, and consequently a 3 determination is made which is adverse to the individual; or fails to comply with any other provision or rule promulgated there under, in such a way as to have an adverse effect on an individual, the individual may bring a civil action against the agency, and the district

courts of the United States shall have jurisdiction in the matters under the provisions of this subsection.

b. When an individual or agency who knowingly and/or willingly maintains a SOR without a relevant and necessary need to accomplish a purpose of the agency required to be accomplished by statute or by executive order of the President; fails to inform each individual whom it asks to supply information, on a form which it uses to collect the information or on a separate form that can be retained by the individual: the authority (whether granted by statute, or by executive order of the President) which authorizes the solicitation of the information and whether the disclosure of such information is mandatory or voluntary; the principal purpose or purposes for which the information is intended to be used; the routine uses which may be made of the information, as published pursuant to paragraph (4)(D) of the Privacy Act; the effects on him/her, if any, of not providing all or any part of the requested information.

Privacy Advisory—A statement required when soliciting personally-identifying information that is not maintained in a SOR. The Privacy Advisory informs the individual why the information is being solicited and how it will be used.

Privacy Impact Assessment—A written assessment of an information system that addresses the information to be collected, the purpose and intended use; with whom the information will be shared; notice or opportunities for consent to individuals; how the information will be secured; and whether a new SOR is being created under the Privacy Act.

Program Manager (PM)—The individual specifically designated to be responsible for the life cycle management of a system or end item. The PM is vested with full authority, responsibility, and resources to execute and support an approved AF program. The PM is accountable for credible cost, schedule, and performance reporting to the Milestone Decision Authority (DoD 5000.01). Throughout this document the term "Program Manager" is used for consistency with DoD policy and documentation.

Public or Person—(as defined in 5 CFR 1320) Members of the public, or the term "person," include individuals, partnerships, associations, corporations (including government-owned contractor-operated [GOCO] facilities), business trusts, legal representatives, organized group of individuals, state, territory, or local government.

Routine Use—A disclosure of records to individuals or agencies outside DoD for a use that is compatible with the purpose for which the AF created the records.

Sensitive Information—Public Law 100-235, *The Computer Security Act of 1987* established requirements for protection of certain information in U.S. Government automated information systems (AIS). This information is referred to as "sensitive" information, defined in the Act as: "Any information, the loss, misuse, or unauthorized access to or modification of which could adversely affect the national interest or the conduct of Federal programs, or the privacy to which individuals are entitled under section 552a of title 5, United States Code (the Privacy Act), but which has not been specifically authorized under criteria established by an Executive order or an Act of Congress to be kept secret in the interest of national defense or foreign policy."

System Manager—The official who is responsible for managing a SOR including guidance and procedures to operate and safeguard it. Local system managers operate record systems or are responsible for part of a decentralized system whether paper or electronic.

System Notice—See System of Records Notice (SORN).

System of Records—A group of records under the control of a DoD Component from which an individual's record is retrieved by the name or personal identifier.

System of Records Notice (SORN) /or/ Privacy Act System Notice—The official public notice published in the *Federal Register* of the existence, content, and Points of Contact for the SOR containing Privacy Act data.

Third Party Requester—A request from any person for access to another individual's Privacy Act record without that individual's written consent.

Attachment 2

PREPARING A SYSTEM OF RECORDS NOTICE (SORN)

A2.1. The following elements comprise a SORN for publication in the Federal Register: *(For examples see Privacy website Helpful Resources,* **http://www.privacy.af.mil/helpfulresources/index.asp**).

A2.2. System Identifier. AF Privacy Office, SAF/A6PP assigns the notice number, for example, F033 AF PC A, where "F" indicates "Air Force," the next number represents the publication series number related to the subject matter, and the final letter group shows the system manager's command or Deputy Chief of Staff (DCS). The last character "A" indicates that this is the first notice for this series and system manager.

A2.3. System Name. Use a short, specific, plain-language title that identifies the system's general purpose (limited to 55 characters).

A2.4. System Location. Specify the address of the primary system and any decentralized elements, including automated data systems with a central computer facility and input or output terminals at separate locations. Use street address, 2-letter state abbreviations and 9-digit ZIP Codes. Spell out office names. Do not use office symbols.

A2.5. Categories of Individuals Covered by the System. Use nontechnical, specific categories of individuals about whom the AF keeps records. Do not use categories like "all AF personnel" unless they are actually true.

A2.6. Categories of Records in the System. Describe in clear, plain language, all categories of records in the system. List only documents actually kept in the system. Do not show source documents that are used to collect data and then destroyed. Do not list form numbers.

A2.7. Authority for Maintenance of the System. Cite the specific law or executive order that authorizes the program the record supports. **Note**: EO 9397 (SSN), as amended, authorizes, but does require the use of the SSN as a personal identifier. It has been amended by EO 13478. Include both executive orders as authority whenever the SSN is collected and/or used to retrieve records.

A2.8. Purpose. Describe briefly and specifically what the AF does with the information collected.

A2.9. Routine Uses of Records Maintained in the System Including Categories of Users and the Purpose of Such Uses. List each specific agency or activity outside DoD to whom the records may be released and the purpose for such release. The DoD 'Blanket Routine Uses' published in the AF Directory of System Notices apply to all system notices.

A2.10. Guidance for Storing, Retrieving, Accessing, Retaining, and Disposing of Records in the System:

A2.10.1. **Storage.** State the medium in which the AF keeps the records; for example, in file folders, card files, microfiche, computer, or a combination of those methods. Storage does not refer to the storage container.

A2.10.2. **Retrievability.** State how the AF retrieves the records; for example, by name, SSN, or personal characteristics (such as fingerprints or voiceprints).

A2.10.3. **Safeguards.** List the kinds of officials who have immediate access to the system. List those responsible for safeguarding the records. Identify the system safeguards; for example, storage in safes, vaults, locked cabinets or rooms, use of guards, visitor controls, personnel screening, computer systems software, and so on. Describe safeguards fully without compromising system security.

A2.10.4. **Retention and Disposal.** State how long the activity must maintain the record IAW its approved Records Disposition. Indicate if or when the records may be transferred to a Federal Records Center and how long the record stays there. Specify when the Records Center transfers legal ownership of (accession) the record to the National Archives or when the Records center destroys the record. Indicate how the records may be destroyed. Consult with your Records Professional on finding an appropriate disposition in the AF Records Disposition Schedule in AFRIMS, **https://www.my.af.mil/afrims/afrims/afrims/rims.cfm**.

A2.11. System Manager and Address. List the position title and duty address of the system manager. For decentralized systems, show the locations and the position or duty title of each category of officials responsible for any segment of the system.

A2.12. Notification Procedure. List the title and duty address of the official authorized to tell requesters if their records are in the system. Specify the information a requester must submit; for example, full name, military status, SSN, date of birth, or proof of identity, and so on.

A2.13. Record Access Procedures. Explain how individuals may arrange to access their records. Include the titles or categories of officials who may assist; for example, the system manager.

A2.14. Contesting Records Procedures. SAF/A6PPF provides this standard caption.

A2.15. Record Source Categories. Show categories of individuals or other information sources for the system.

A2.16. Exemptions Claimed for the System. When a system has no approved exemption, write "None" under this heading. Specifically list any approved exemption including the subsection in the Act.

Attachment 3

DOD BLANKET ROUTINE USE

The DoD 'BLANKET ROUTINE USES' are at http://dpclo.defense.gov/privacy/SORNs/blanket_routine_uses.html.

A3.1. DoD Blanket Routine Uses. Certain DoD 'blanket routine uses' have been established that are applicable to every record system maintained by the Department of the Air Force, unless specifically stated otherwise within the particular record system notice. These additional routine uses of the records are published only once in the Air Force's Preamble to its compilation of records systems in the interest of simplicity, economy and to avoid redundancy. Updates and current versions of the DoD Blanket Routine uses are maintained on the DPCLO website.

A3.2. Law Enforcement Routine Use. If a system of records maintained by a DoD Component to carry out its functions indicates a violation or potential violation of law, whether civil, criminal, or regulatory in nature, and whether arising by general statute or by regulation, rule, or order issued pursuant thereto, the relevant records in the system of records may be referred, as a routine use, to the agency concerned, whether federal, state, local, or foreign, charged with the responsibility of investigating or prosecuting such violation or charged with enforcing or implementing the statute, rule, regulation, or order issued pursuant thereto.

A3.3. Disclosure when Requesting Information Routine Use. A record from a system of records maintained by a Component may be disclosed as a routine use to a federal, state, or local agency maintaining civil, criminal, or other relevant enforcement information or other pertinent information, such as current licenses, if necessary to obtain information relevant to a Component decision concerning the hiring or retention of an employee, the issuance of a security clearance, the letting of a contract, or the issuance of a license, grant, or other benefit.

A3.4. Disclosure of Requested Information Routine Use. A record from a system of records maintained by a Component may be disclosed to a federal agency, in response to its request, in connection with the hiring or retention of an employee, the issuance of a security clearance, the reporting of an investigation of an employee, the letting of a contract, or the issuance of a license, grant, or other benefit by the requesting agency, to the extent that the information is relevant and necessary to the requesting agency's decision on the matter.

A3.5. Congressional Inquiries Routine Use. Disclosure from a system of records maintained by a Component may be made to a congressional office from the record of an individual in response to an inquiry from the congressional office made at the request of that individual.

A3.6. Private Relief Legislation Routine Use. Relevant information contained in systems of records of the Department of Defense published on or before August 22, 1975, will be disclosed to the Office of Management and Budget in connection with the review of private relief legislation as set forth in Office of Management and Budget Circular A-19 at any stage of the legislative coordination and clearance process as set forth in that Circular.

A3.7. Disclosures Required by International Agreements Routine Use. A record from a system of records maintained by a Component may be disclosed to foreign law enforcement, security, investigatory, or administrative authorities to comply with requirements imposed by, or to claim rights conferred in, international agreements and arrangements including those regulating the stationing and status in foreign countries of DOD military and civilian personnel.

A3.8. Disclosure to State and Local Taxing Authorities Routine Use. Any information normally contained in Internal Revenue Service (IRS) Form W-2 which is maintained in a record from a system of records maintained by a Component may be disclosed to state and local taxing authorities with which the Secretary of the Treasury has entered into agreements under 5 U.S.C., sections 5516, 5517, and 5520 and only to those state and local taxing authorities for which an employee or military member is or was subject to tax regardless of whether tax is or was withheld. This routine use is in accordance with Treasury Fiscal Requirements Manual Bulletin No. 76-07.

A3.9. Disclosure to the Office of Personnel Management Routine Use. A record from a system of records subject to the Privacy Act and maintained by a Component may be disclosed to the Office of Personnel Management (OPM) concerning information on pay and leave, benefits, retirement deduction, and any other information necessary for the OPM to carry out its legally authorized government-wide personnel management functions and studies.

A3.10. Disclosure to the Department of Justice for Litigation Routine Use. A record from a system of records maintained by this component may be disclosed as a routine use to any component of the Department of Justice for the purpose of representing the Department of Defense, or any officer, employee or member of the Department in pending or potential litigation to which the record is pertinent.

A3.11. Disclosure to Military Banking Facilities Overseas Routine Use. Information as to current military addresses and assignments may be provided to military banking facilities who provide banking services overseas and who are reimbursed by the Government for certain checking and loan losses. For personnel separated, discharged, or retired from the Armed Forces, information as to last known residential or home of record address may be provided to the military banking facility upon certification by a banking facility officer that the facility has a returned or dishonored check negotiated by the individual or the individual has defaulted on a loan and that if restitution is not made by the individual, the U.S. Government will be liable for the losses the facility may incur.

A3.12. Disclosure of Information to the General Services Administration (GSA) Routine Use. A record from a system of records maintained by this component may be disclosed as a routine use to the General Services Administration (GSA) for the purpose of records management inspections conducted under authority of 44 U.S.C. 2904 and 2906.

A3.13. Disclosure of Information to the National Archives and Records Administration (NARA) Routine Use. A record from a system of records maintained by this component may be disclosed as a routine use to the National Archives and Records Administration (NARA) for the purpose of records management inspections conducted under authority of 44 U.S.C. 2904 and 2906.

A3.14. Disclosure to the Merit Systems Protection Board Routine Use. A record from a system of records maintained by this component may be disclosed as a routine use to the Merit Systems Protection Board, including the Office of the Special Counsel for the purpose of litigation, including administrative proceedings, appeals, special studies of the civil service and other merit systems, review of OPM or component rules and regulations, investigation of alleged or possible prohibited personnel practices; including administrative proceedings involving any individual subject of a DoD investigation, and such other functions, promulgated in 5 U.S.C. 1205 and 1206, or as may be authorized by law.

A3.15. Counterintelligence Purpose Routine Use. A record from a system of records maintained by this component may be disclosed as a routine use outside the DoD or the U.S. Government for the purpose of counterintelligence activities authorized by U.S. Law or Executive Order or for the purpose of enforcing laws, which protect the national security of the United States.

Attachment 4

ALTERING A SYSTEM OF RECORD NOTICE

A4.1. A system is considered altered.

Table A4.1. Criteria for altering a System of Records Notice.

Alterations	DoD 5400.11-R Citation	DoD 5400.11-R Exclusions
Categories of Individuals: C6.4.2.1. A significant increase or change in the number or type of individuals about whom records are maintained.	C6.4.2.1.1. Only changes that alter significantly the character and purpose of the record system are considered alterations.	C6.4.2.1.2. Increases in numbers of individuals due to normal growth are not considered alterations unless they truly alter the character and purpose of the system.
	C6.4.2.1.3. Increases that change significantly the scope of population covered.	C6.4.2.1.4. A reduction in the number of individuals covered is not an alteration, but only an amendment.
	C6.4.2.1.5. All changes that add new categories of individuals to system coverage require a change to the "Categories of individuals covered by the system" caption of the notice	
Categories of Records: C6.4.2.2. An expansion in the types or categories of information maintained.	C6.4.2.2.3. All changes under this criterion require a change to the "Categories of Records in the System" caption of the notice.	
Retrievability: C6.4.2.3. An alteration of how the records are organized or the manner in which the records are indexed and retrieved.	C6.4.2.3.2. Any change under this criterion requires a change in the "Retrievability" caption of the system notice.	
	C6.4.2.3.3. If the records are no longer retrieved by name or personal identifier, cancel the system notice.	
Purpose: C6.4.2.4. A change in the purpose for which the information in the system is used.	C6.4.2.4.1. The new purpose must not be compatible with the existing purposes for which the system is maintained.	C6.4.2.4.2. If the use is compatible and reasonably expected, there is no change in purpose and no alteration occurs.
	C6.4.2.4.3. Any change under this criterion requires a change in the	

Alterations	DoD 5400.11-R Citation	DoD 5400.11-R Exclusions
	"Purpose(s)" caption (see paragraph C6.3.8. of this Chapter) and may require a change in the "Authority for maintenance of the system" caption (see paragraph C6.3.7. of this Chapter).	
Location:	C6.4.2.5.1. Increasing the number of offices with direct access is an alteration.	
Combining system of records:	C6.4.2.3.1. The change must alter the nature of use or scope of the records involved (for example, combining records systems in reorganization).	
Computer Environment: C.6.4.2.5. Changes that alter the computer environment (such as, changes to equipment configuration, software, or procedures) so as to create the potential for greater or easier access	C6.4.2.5.2. Software applications, such as operating systems and system utilities, which provide for easier access, are considered alterations.	
	C6.4.2.5.3. The addition of an on-line capability to a previously batch-oriented system is an alteration.	
	C6.4.2.5.4. The addition of peripheral devices such as, tape devices, disk devices, card readers, printers, and similar devices to an existing IT system constitute an amendment if system security is preserved.	
Storage:	C6.4.2.5.6. The connecting of two or more formerly independent automated systems or networks together creating a potential for greater access is an alteration.	
	C6.4.2.5.7. Any change under this caption requires a change to the "Storage" caption element of the systems notice.	

Attachment 5

RISK ASSESSMENT

A5.1. Risk Notification. Five factors are used when determining if an agency is required to notify those who may have been affected by a PII breach. Agencies should take the time to determine the risk of harm, embarrassment, inconvenience or unfairness surrounding the breach. The factors used in assessing the likely risk of harm are:

A5.1.1. Nature of Data Elements Breached**.** Consider context of the data involved and the potential harm, embarrassment, inconvenience or unfairness that might be generated by its exposure to unauthorized individuals.

A5.1.2. Number of Individuals Affected**.** The magnitude of the number of individuals affected may determine how they will be notified, but should not impact an agency's decision to provide notification.

A5.1.3. Likelihood the Information is Accessible and Useable**.** Upon discovery of a breach, agencies should assess the likelihood the personally identifiable information has been or will be used by unauthorized individuals. The greater the risk that the information may be used unlawfully should influence an agency's decision to provide notification to the individual(s).

A5.1.4. Likelihood the breach may lead to harm, embarrassment, inconvenience or unfairness to an individual.

A5.1.4.1. Broad Reach of Potential Harm, **Embarrassment, Inconvenience or Unfairness.** Consider the possible harm associated with the loss or compromise of the PII, i.e., loss of self- esteem, mental pain or emotional stress.

A5.1.4.2. Likelihood Harm, **Embarrassment, Inconvenience or Unfairness Will Occur.** Agencies must determine the type of data has been compromised and the manner the breach occurred.

A5.1.5. **Ability of the Agencies to Mitigate the Risk of Harm, Embarrassment, Inconvenience or Unfairness.** In addition to containing the breach, agencies must determine what countermeasures will be used to prevent further compromise of the system's PII.

Attachment 6

PREPARING A DOD SSN JUSTIFICATION MEMORANDUM

MEMORANDUM THRU AIR FORCE PRIVACY OFFICE, SAF/A6PPF

FOR DIRECTOR FOR PRIVACY, DPCLO

SUBJECT: Justification for the Use of the Social Security Number (SSN)

The memorandum should begin by naming the DITPR number of the IT system and/or form that is the subject of the justification. The description must be sufficiently detailed so that someone unfamiliar with the system can grasp the general understanding of its intent.

The justification for the use of the SSN must include a reference to the SSN Instruction Use Case that is being used to justify the use of the SSN. If the justification does not fall under either the operational necessity use case or the legacy system interface use case, then the justification shall also include the specific reference to the law that requires the use of the SSN and why it is applicable to the use being justified.

Reference is made to the system or form supporting documentation, including but not limited to, System of Records Notice (SORN), Privacy Impact Assessment (PIA), Paperwork Reduction Act (PRA) notice, or any other documentation that may be appropriate. If the substance of the documentation is not attached, reference is made to how the reader may gain access to this documentation.

Justification for the use of the SSN does not constitute blanket permission to use the SSN. Specific reference shall be made to indicate actions being taken to reduce the vulnerability of SSNs, which may include indicating where SSNs are being removed from transactions, where SSNs are no longer displayed, or any other protections that have been included. It should be obvious to the reader that a thorough effort has been made to evaluate the risk associated with the system or form and that every reasonable step has been or is being taken to reduce the use of the SSN and protect it where the use is still required.

If the justification for the use of the SSN falls under the “legacy use” authorization and is not specifically required by the law, reference shall be made to the Plan of Actions and Milestones for the elimination of the use of the SSN.

Official’s Name
GENERAL/SES

Attachment 7

EXAMPLE PRIVACY BREACH NOTIFICATION LETTER

OFFICIAL LETTERHEAD

Dear Mr. John Miller:

On January 1, 2006, a DoD laptop computer was stolen from the parked car of a DoD employee in Washington, D.C. after normal duty hours while the employee was running a personal errand. The laptop contained personally identifying information on 100 DoD employees who were participating in the xxx Program. The compromised information is the name, social security number, residential address, date of birth, office and home e-mail address, office, and home telephone numbers of the Program participants.

The theft was immediately reported to local and DoD law enforcement authorities, who are now conducting a joint inquiry into the loss.

We believe that the laptop was the target of the theft as opposed to any information that the laptop might contain. Because the information in the laptop was password protected and encrypted, we also believe that the probability is low that the information will be acquired and used for an unlawful purpose. However, we cannot say with certainty that this might not occur. We therefore believe that you should consider taking such actions to protect yourself against the potential that someone might use the information to steal your identity.

You should be guided by the actions recommended by the Federal Trade Commission (FTC) on its Web site at http://www.consumer.ftc.gov/articles/0275-place-fraud-alert. The FTC urges that you to immediately place an initial fraud alert on your credit file. The fraud alert is for a period of 90 days, during which, creditors are required to contact you before a new credit card is issued or an existing card changed. The site also provides other valuable information that can be taken now or in the future if problems should develop.

The Department of Defense takes this loss very seriously and is reviewing its current policies and practices with a view of determining what must be changed to preclude a similar occurrence in the future. At a minimum, we will be providing additional training to personnel to ensure that they understand that personally identifiable information must at all times be treated in a manner that preserves and protects the confidentiality of the data.

We deeply regret and apologize for any inconvenience and concern this theft may cause you.

Should you have any questions, please call _____.

Sincerely,
Signature Block
(Directorate level or higher)

Attachment 8

APPROVED DOD TRAINING WEBSITES

Approved DoD Privacy Training Websites

Portable Electronic Devices and Removable Storage Media V2.0, The new Portable Electronic Devices (PED) training is now available online:

http://iase.disa.mil/eta/pedrm_v2/pedrm_v2/launchPage.htm

The new Social Networking training is now available online:

http://iase.disa.mil/eta/sns_v1/sn/launchPage.htm

DoD Social Media Hub Education and Training website:

http://www.defense.gov/socialmedia/education-and-training.aspx/

Attachment 9

NATIONAL COMPLAINT VIGNETTES

Disclaimer: Vignettes are provided for the instructional purpose of teaching how to identify Civil Liberties related issues only. They do not reflect official policies or positions of the Department of Defense.

1. Religion.

a. Scenario: During the work day, a military unit attended a religious themed movie at the base theater. Members were given the choice of watching the movie or cleaning the barracks while the unit watched the movie. A week later a member of the unit submitted a complaint. In his complaint, he said he chose to watch the movie because he viewed cleaning the barracks as punishment, but now he feels like his religious freedom was violated. He does not think a punishment, like cleaning the barracks, should be an alternative to watching a religious themed movie.

b. Civil Liberties Issue: First Amendment; Freedom of Religion. A service member should not be punished for participating or not participating in a religious activity. If the service member's belief that he faced a punishment for not attending the movie is accurate, his unit leadership should be counseled about the necessity of allowing for unit member religious freedom without the threat of punishment.

2. Social Media Use & Operational Security.

a. Scenario: A deployed service member posted a photograph on Facebook. The caption indicated that his team had just returned from a patrol, and the date/time stamp on the photo showed exactly when it was taken. The service member's chain of command told him to take down the photograph, to protect operational security. However, the service member stated that he was using his personal Facebook account, during his personal time (not while on duty), and not claiming to represent or speak for the military.

b. Civil Liberties Issue: Freedom of Speech/Expression. While individuals have a right to express themselves through online social media outlets, such expression must not compromise operational security. DTM 09-026, "Responsible and Effective Use of Internet-based Capabilities," Attachment 2, section 5, states that "when accessing Internet-based capabilities using Federal Government resources in an authorized personal or unofficial capacity, individuals shall employ sound operations security (OPSEC) measures." Other regulations, like the "Joint Ethics Regulation and the Standards of Ethical Conduct for Employees of the Executive Branch," prohibit the release of non-public information, require appropriate disclaimers of opinions being expressed, and restrict the use of government computers to access and to manage personal sites during official duty time.

3. Service Members' Political Involvement.

a. Scenario: An active-duty service member placed a bumper sticker on his privately owned vehicle. The chain of command told the service member to remove the sticker, but the service member refused, citing his Constitutional right to freedom of speech and freedom of expression.

b. Civil Liberties Issue: Freedom of Speech/Expression/Assembly (to the extent that showcasing one's political affiliation constitutes assembly). In keeping with the traditional concept that service members on active duty should not engage in partisan political activity, and that service members not on active duty should avoid inferences that their political activities imply or appear to imply official sponsorship, approval, or endorsement, the military may regulate service members' participation in political activities. According to DoDD1344.10, Sec 4.1.1.8. "A member of the Armed Forces on active duty may: display a political bumper sticker on the member's private vehicle." In this case, the Directive regulating such participation allows the service member to display the bumper sticker. Unit leadership should be counseled about DoD policies regulating service members' participation in political activities.

4. Search and Seizure.

a. Scenario: A DoD civilian, employed at a CONUS Air Force base, was randomly selected to have his vehicle searched at the gate. The gate guard inspected the engine compartment, exterior and undercarriage of the vehicle, and the interior of the vehicle, including the glove box and consoles. The employee submitted a complaint to the base Civil Liberties Officer, alleging that a search of the glove box and consoles was excessive and unreasonable.

b. Civil Liberties Issue: Right to be Secure against Unreasonable Searches and Seizures. Installation commanders issue regulations for the protection and security of property or places under their command. The search followed established procedures for vehicle searches, per guidance provided in Air Force Instruction 31-204 "Air Force Motor Vehicle Traffic Supervision." In evaluating this type of case, consider whether a command authorizes the search of glove boxes and consoles. For example, the AFI instructs officials conducting searches of vehicles entering a military installation to "look under all seats, under/behind dash, glove box, consoles, visors, ashtrays and any packages and briefcases."

5. Don't Ask, Don't Tell – With Speech/Religion Implications.

a. Scenario: A service member speaks with a friend, informally on base, about the repeal of Don't Ask, Don't Tell. The service member, consistent with her religion, expressed opposition to homosexuality. The service member's senior overheard comments and told her to stop expressing these views on base. The service member filed a Civil Liberties complaint, alleging that her freedom of speech/religion was violated when she was told to stop expressing her religious views on base.

b. Civil Liberties Issue: Freedom of Speech/Religion. Service members may express moral or religious beliefs, so long as service members do NOT make statements detrimental to good order and discipline, and so long as service members obey lawful orders. Whether or not the service member's Civil Liberties were, in fact, violated is dependent upon whether or not her comments fall within the constraints articulated in the guidance above.

6. Carrying Privately Owned Weapons on Military Installations.

a. Scenario: Service member living in family housing aboard a Marine Corps base is required to report to the Provost Marshall that she possesses a firearm and stores it at her home. The service member filed a complaint with the Civil Liberties POC arguing that the Provost Marshall should not be keeping records on how she exercises her right to keep and bear arms.

b. Civil Liberties Issue: Right to Keep and Bear Arms. In reviewing the service member's complaint, consider whether the PM's requirement to report the firearm is authorized by a base order or other regulation.

7. Civilian Employment Complaint.

a. Scenario: A DoD civilian supervisor typically allows overtime for all employees who volunteer. However, a civilian employee in that office submitted a complaint, alleging that he has not been allowed to work overtime because the supervisor saw him at an anti-war protest on a Saturday last year. His complaint letter alleged that because his supervisor will not allow him to work overtime, his Civil Liberties are being violated.

b. Civil Liberties Issue: Right to Due Process. His complaint about not being allowed to work overtime, when other workers are encouraged to work overtime, could be a recognized employee grievance. Direct him to consider the use of his agency's existing employee grievance process.

8. Member of Public, Pentagon Protests, and Suspicious Activity Reporting.

a. Scenario: A member of the public attended a protest at the Pentagon. He followed all rules and procedures governing the protest, including not making threatening statements or displaying threatening behavior, and complied with instructions from Pentagon Police Officers. The individual submitted a complaint alleging that a civilian employee, employed at the Pentagon, asked each of the protestors to identify themselves and subsequently stated that he was going to identify them in a suspicious activity report, due to their participation in the protest.

b. Civil Liberties Issue: Freedom of Speech, Peaceable Assembly. Consider whether the Privacy Act of 1974 is implicated by the Pentagon employee’s actions. According to the Privacy Act (5 U.S.C. § 552a(e)(7)), “no information shall be maintained on how an individual exercises rights protected by the First Amendment to the Constitution of the United States, including the freedoms of speech, assembly, press and religion, except as follows:

i. When specifically authorized by statute.

ii. When expressly authorized by the individual, group of individuals, or association on whom the record is maintained.

iii. When the record is pertinent to and within the scope of an authorized law enforcement activity.”

Attachment 10

CIVIL LIBERTIES COMPLAINT REPORT INSTRUCTIONS

Introduction

Section 803 of Public Law 110-53 requires the Department to report its Civil Liberties activities to Congress. In order to comply with that requirement, each DoD Component must submit a quarterly report to the Defense Privacy and Civil Liberties Office (DPCLO). DPCLO will consolidate Component data and submit the Department's reports to Congress.
Component reports must include the following:

(1) The number and nature of Civil Liberties complaints received; and
(2) A summary of the disposition of such complaints.

Quarterly reports are due by the 10th day of the month following the closing of each fiscal year quarter to the AF Civil Liberties POC: afcivil.Liberties@pentagon.af.mil.

Component Points of Contact (POCs) Reporting Responsibilities

POCs are responsible for establishing procedures to report Civil Liberties complaints for their entire Component.

To ensure the Department is accurately accounting for and addressing Civil Liberties complaints, Component reporting procedures should capture Civil Liberties complaints that may be received by offices such as the Inspector General (IG), Equal Employment Opportunity (EEO), and Labor Management Employee Relations (LMER). Component reporting procedures should also ensure that there is no duplicate reporting within the Component.

Report Guidance

Definitions

Civil Liberties Complaint:
For purposes of reporting, a complaint is an allegation of one or more Civil Liberties violations.

Received:
The Component has received the complaint and is evaluating it for a Civil Liberties implication.

Pending:
The complaint has **not** been fully adjudicated or resolved.

Resolved:
The complaint has been fully adjudicated or resolved.
Provide a summary of complaints on a separate sheet of paper. Include the following information for each complaint:

1. Description of complaint. Please identify the constitutional amendment, law, regulation, or other authority alleged to be violated in the complaint, if possible.

Do not include any personally identifiable information (PII) about the complainant or any other persons involved in complaint (examples of PII include names, addresses, phone numbers, and Social Security Numbers).

2. Findings; and

3. Disposition.

Examples of Potential Complaints Implicating Civil Liberties (not an exhaustive list):
A military service member claims he was punished by his commanding officer for refusing to attend a religious activity; or by not being allowed to attend a religious function in accordance with his religious beliefs.

A civilian employee made disparaging comments about the Department via his personal social networking page and was instructed by his supervisor to remove the posts, or be reprimanded.

Attachment 11

EXAMPLE CIVIL LIBERTIES REPORT

SUMMARY OF CIVIL LIBERTIES COMPLAINTS

3RD QTR FY11 – APRIL TO JUNE 2011

DEPARTMENT OF THE AIR FORCE

TOTAL NUMBER OF COMPLAINTS: 2

Complaint #1:

Description of Complaint: Complainant alleges his new supervisor sent an e-mail to all-hands announcing that the pre-existing practice of allowing employees to take time away from their desks for religious prayer is being discontinued. Possible First Amendment, Freedom of Religion implication.

Findings: The Department of the Air Force has received and evaluated the complaint, and the complaint is being investigated.

Disposition: Pending.

Complaint #2:

Description of Complaint: Complainant alleges he was reprimanded for attending a political rally during his lunch break. Possible First Amendment, Freedom of Association implication.

Findings: The Department of the Army has received and evaluated the complaint, and the complaint is being investigated.

Disposition: Pending.